



MaxiiNet™ VI3026

Operational Manual

**20 GE PoE-Plus + 4 GE PoE-Plus Combo SFP + 2 GE SFP L2
26 Port Managed Switch**

Release 2.44

About This Manual

Copyright

Copyright © 2013 Vigitron, Inc. All rights reserved. The products and programs described in this User's Manual are licensed products of Vigitron Inc. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted. No parts of this User's Manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. This includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.

Purpose

This Manual gives specific information on how to operate and use the management functions of the Vi3026.

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used throughout this guide to show information:



NOTE: Emphasizes important information or calls your attention to related features or instructions.



WARNING: Alerts you to a potential hazard that could cause personal injury.



CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to your manufacture products and replacement parts can be obtained from Vigitron, Inc.

Disclaimer

Vigitron, Inc. does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this User's Manual. Vigitron makes no commitment to update or keep current the information in this User's Manual, and reserves the rights to make improvements to this User's Manual and /or to the products described in this

User's Manual, at any time without notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the CE/FCC remove Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Caution

To assure continued compliance (example: use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class A device. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

UL Mark



UL 60950-1 Information Technology Equipment - Safety - Part 1:
General Requirements - Edition 2 - Revision Date 2014/05/13

Contents

About This Manual	2
Introduction.....	10
Overview	10
Chapter 1: Operation of Web-Based Management.....	11
Connecting Network Devices	14
Twisted-Pair Devices	14
Cabling Guidelines	14
Chapter 2: System Configuration.....	16
2-1 System Information.....	16
2-1.1 Information	16
2-1.2 Configuration	18
2-2 Time	19
2-2.1 Manual	19
2-2.2 NTP.....	21
2-3 Account	22
2-3.1 Users	22
2-3.2 Privilege Level	24
2-4 IP	26
2-4.1 IPv4	26
2-4.2 IPv6	28
2-5 Syslog	29
2-5.1 Configuration	29
2-5.2 Log.....	30
2-5.3 Detailed.....	31
2-6 SNMP	32
2-6.1 System.....	32
2-6.2 Configuration	33
2-6.3 Communities.....	34
2-6.4 Users	35
2-6.5 Groups.....	37
2-6.6 Views.....	38
2-6.7 Access.....	39
2-6.8 Trap	41
Chapter 3: Configuration.....	43
3-1 Port	43

3-1.1 Configuration	43
3-1.2 Port Description	46
3-1.3 Traffic Overview	47
3-1.4 Detailed Statistics	48
3-1.5 QoS Statistics	50
3-1.6 SFP Information	51
3-1.7 EEE	53
3-2 ACL	55
3-2.1 Ports	55
3-2.2 Rate Limiters	57
3-2.3 Access Control List	58
3-2.4 ACL Status	67
3-3 Aggregation	69
3-3.1 Static Trunk	69
3-3.2 LACP	71
3-4 Spanning Tree	76
3-4.1 Bridge Settings	76
3-4.2 MSTI Mapping	79
3-4.3 MSTI Priorities	81
3-4.4 CIST Ports	82
3-4.5 MSTI Ports	84
3-4.6 Bridge Status	86
3-4.7 Port Status	87
3-4.8 Port Statistics	88
3-5 IGMP Snooping	89
3-5.1 Basic Configuration	89
3-5.2 VLAN Configuration	91
3-5.3 Port Group Filtering	93
3-5.4 Status	95
3-5.5 Group Information	97
3-5.6 IPv4 SSM Information	98
3-6 MLD Snooping	100
3-6.1 Basic Configuration	100
3-6.2 VLAN Configuration	103
3-6.3 Port Group Filtering	105
3-6.4 Status	106
3-6.5 Group Information	108

3-6.6 IPv6 SSM Information	109
3-7 MVR	110
3-7.1 Configuration	110
3-7.2 Port Group Allow.....	112
3-7.3 Groups Information.....	113
3-7.4 Statistics	114
3-8 LLDP	115
3-8.1 LLDP Configuration.....	115
3-8.2 LLDP Neighbours	118
3-8.3 LLDP-MED Configuration.....	120
3-8.4 LLDP-MED Neighbours	125
3-8.5 EEE	128
3-8.6 Port Statistics	130
3-9 PoE	132
3-9.1 Configuration	132
3-9.2 Status	134
3-9.3 Power Delay	136
3-9.4 Auto Checking	138
3-9.5 Scheduling.....	140
3-10 Filtering Data Base	141
3-10.1 Configuration	141
3-10.2 Dynamic MAC Table	144
3-11 VLAN	145
3-11.1 VLAN Membership	145
3-11.2 Ports	147
3-11.3 Switch Status.....	149
3-11.4 Port Status.....	151
3-11.5 Private VLANs.....	153
3-11.6 MAC-Based VLAN	155
3-11.7 Protocol-Based VLAN	158
3-12 Voice VLAN.....	162
3-12.1 Configuration	162
3-12.2 OUI	164
3-13 GARP	165
3-13.1 Configuration	165
3-13.2 Statistics	167
3-14 GVRP	168

3-14.1 Configuration	168
3-14.2 Statistics	170
3-15 QoS	171
3-15.1 Port Classification.....	171
3-15.2 Port Policing	174
3-15.3 Port Scheduler.....	176
3-15.4 Port Shaping	179
3-15.5 Port Tag Remarking	182
3-15.6 Port DSCP	184
3-15.7 DSCP-Based QoS	186
3-15.8 DSCP Translation	188
3-15.9 DSCP Classification	190
3-15.10 QoS Control List Configuration.....	191
3-15.11 QCL Status	195
3-15.12 Storm Control.....	197
3-16 S-Flow Agent	198
3-16.1 Collector	198
3-16.2 Sampler	200
3-17 Loop Protection	202
3-17.1 Configuration	202
3-17.2 Status	204
3-18 Single IP.....	205
3-18.1 Configuration	205
3-18.2 Information	206
3-19 Easy Port	207
3-20 Mirroring.....	210
3-21 Trap Event Severity	212
3-22 UPnP	213
Chapter 4: Security	214
4-1 IP Source Guard	214
4-1.1 Configuration	214
4-1.2 Static Table	216
4-1.3 Dynamic Table	217
4-2 ARP Inspection	218
4-2.1 Configuration	218
4-2.2 Static Table	220
4-2.3 Dynamic Table	221

4-3 DHCP Snooping	222
4-3.1 Configuration	222
4-3.2 Statistics	224
4-4 DHCP Relay	226
4-4.1 Configuration	226
4-4.2 Statistics	228
4-5 NAS	230
4-5.1 Configuration	230
4-5.2 Switch Status	238
4-5.3 Port Status.....	240
4-6 AAA	241
4-6.1 Configuration	241
4-6.2 Radius Overview	245
4-6.3 Radius Details	247
4-7 Port Security	251
4-7.1 Limit Control	251
4-7.2 Switch Status	254
4-7.3 Port Status.....	256
4-8 Access Management.....	257
4-8.1 Configuration	257
4-8.2 Statistics	259
4-9 SSH	260
4-10 HTTPs	261
4-11 Auth Method	262
Chapter 5: Maintenance	263
5-1 Restart Device	263
5-2 Firmware.....	264
5-2.1 Firmware Upgrade	264
5-2.2 Firmware Selection	265
5-3 Save/Restore	267
5-3.1 Factory Defaults	267
5-3.2 Save Start	268
5-3.3 Save User.....	269
5-3.4 Restore User.....	270
5-4 Export/Import.....	271
5-4.1 Export Config.....	271
5-4.2 Import Config	272

5-5 Diagnostics	273
5-5.1 Ping	273
5-5.2 Ping6	274
5-6 Battery Replacement	275
Glossary of Web-based Management	276
A	276
C	278
D	278
E	280
F	280
H	281
I	281
L	282
M	283
N	284
O	284
P	285
Q	286
R	286
S	287
T	288
U	288
V	289
Contact Information.....	290

Introduction

Overview

This user's manual will not only tell you how to install and connect your network system, but how to configure and monitor the Vi3026 through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many detailed explanations of hardware and software functions are shown, as well as, the examples of the operation for web-based interface.

The Vi3026 series, the next generation web managed switches from Vigitron, is a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver intelligent features to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications effectively. It provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise application to help you create a more efficient and better-connected workforce.

Vi3026 web managed switches provide 26-ports in a single device. The specifications are highlighted as follows:

- L2+ features provide better manageability, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports.
- Support guest VLAN, voice VLAN, Port based, tag-based and Protocol based VLANs.
- Support 802.3az energy efficient Ethernet standard.
- Support 8K MAC table.
- Support IPv6/ IPv4 dual stack.
- Support s-Flow.
- Support easy-configuration-port for easy implementation of the IP phone, IP camera or wireless environment.

Overview of This User's Manual

- Chapter 1 "Operation of Web-based Management"
- Chapter 2 "System Configuration"
- Chapter 3 "Configuration"
- Chapter 4 "Security"
- Chapter 5 "Maintenance"

Chapter 1: Operation of Web-Based Management

Initial Configuration

This chapter instructs you on how to configure and manage the Vi3026 through the web user interface. With this facility, you can easily access and monitor through any one port of the switch and all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the Vi3026 are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

After the Vi3026 has been finished configuration, you can browse the interface. For instance, if you type <http://192.168.1.1> in the address row in a browser, it will show the following screen and will ask you to input in the username and password in order to login and access authentication.

The default username is “admin” and password is empty. For first time use, please enter the default username and password, and then click the <Login> button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the Vi3026 will not give you a shortcut to username automatically. This looks inconvenient, but it’s the safer option.

The Vi3026 supports a simple user management function to allow only one administrator to configure the system at any one time. *The use of simultaneous administrators could result in unpredictable operation.* Additional users, even with administrator’s identity, should only monitor the system. Those who have no administrator’s identity can only monitor the system. It is suggested, regardless of security level, that viewing is limited to one client at a time. Also, after accessing the Vi3026 and viewing is complete, log out.

Connections involving the input of routers and use of clients accessing servers, the internet, or other networks can result in *a brief disconnection of client's access to the switch GUI*. It is recommended that after programming or monitoring, clients log out and that users without administrator access be allowed only a minimal access period.



NOTE: When you log into the Switch WEB to manage, you must first type the username of the admin. Password is blank. So after you type in the username, please press enter. Management page will enter WEB. When you log into Vi3026 series switch Web UI management, you can use both ipv4 ipv6 login to manage. To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above, or FireFox V1.00 above, and have the resolution 1024x768. The switch supported neutral web browser interface. If the UI is not working with FireFox browser, it might result from PC security system setting.



NOTE: The Vi3026 function enables DHCP, so if you do not have DHCP server to provide IP addresses to the switch, the switch's default IP is 192.168.1.1.

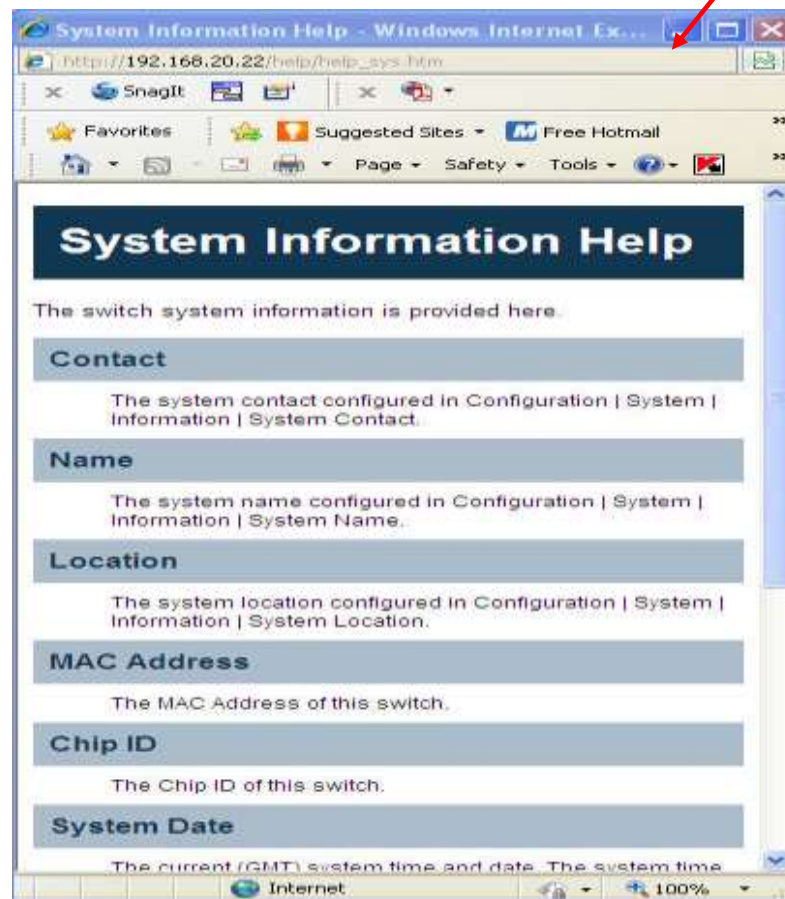
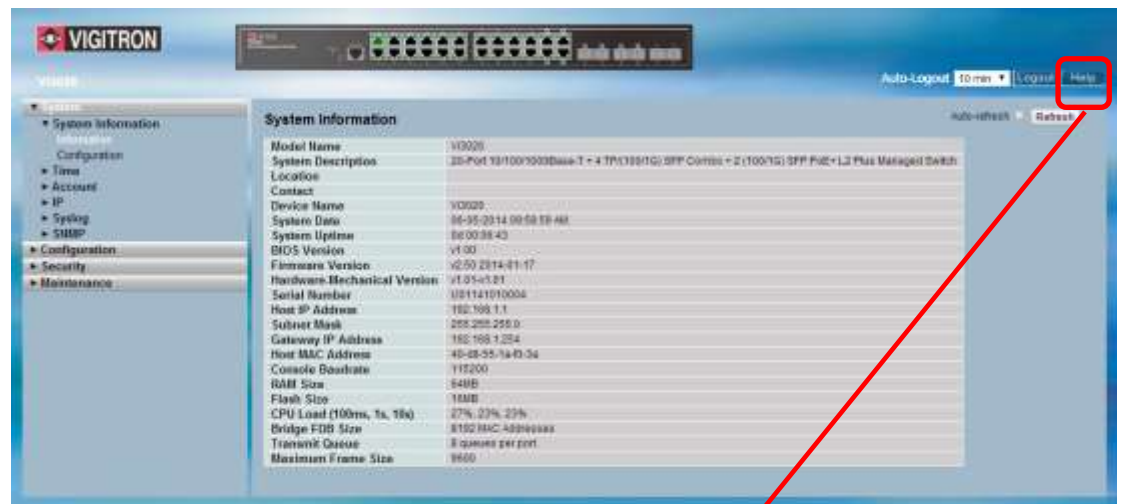


Figure 1: The Login Page



NOTE: If you need to configure the function or parameter, you can refer to the detail in the User Guide. You could also access the switch and click on "help" under the web GUI. The switch will pop up the simple help content to teach you how to set the parameters.

Vi3026 Web Help Function:



Connecting Network Devices

The switch is designed to be connected to 10, 100, or 1,000 Mbps network cards in PCs and servers, as well as, to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e, or 6 cables for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections.

Cabling Guidelines

The RJ-45 ports on the switch support automatic MDI/MDI-X pin-out configuration. You can use standard straight-through twisted-pair cables to connect to any other network devices (E.g. PCs, servers, switches, routers, or hubs).

See Appendix B for further information on cabling.



CAUTION: Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Connecting to PCs, Servers, Hubs and Switches

Step 1: Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

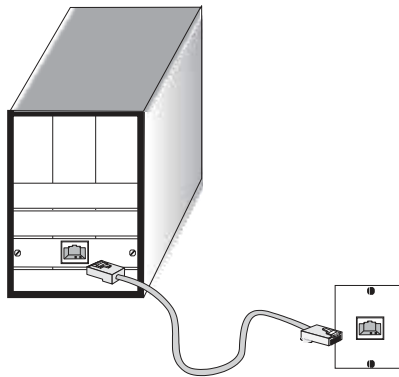


Figure 16: Making Twisted-Pair Connections

Step 2: If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet (see the section “Network Wiring Connections”). Otherwise, attach the other end to an available port on the switch.

Make sure each twisted pair cable does not exceed 100 meters (328 ft.) in length.



NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Step 3: As each connection is made, the Link LED (on the switch) corresponding to each port will light green (1,000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

Network Wiring Connection

Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows:

Step 1: Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Step 2: If not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located, and the other end to a modular wall outlet.

Step 3: Label the cables to simplify future troubleshooting.

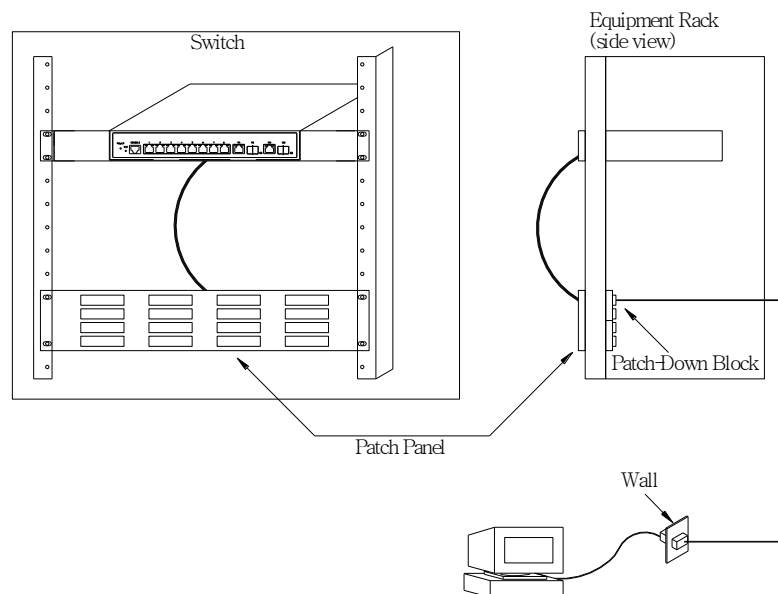


Figure 17: Network Wiring Connections

Chapter 2: System Configuration

2-1 System Information

This chapter describes the entire basic configuration tasks, which includes the System Information and management of the Switch (E.g. Time, Account, IP, Syslog and SNMP).

2-1.1 Information

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Contact”, “Device Name”, “System Up Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size”, “Flash Size” and. With this information, you will know the software version used, MAC address, serial number, how many ports are good and so on. This will be helpful during any malfunctions.

The switch system information is provided here.

Web Interface

To configure System Information in the web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator, as well as, the name and location of the switch. Also, indicate the local time zone by configuring the appropriate offset.
3. Click Refresh.

System Information	
Model Name	Vi3026
System Description	20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP PoE+ L2 Plus Managed Switch
Location	
Contact	
Device Name	Vi3026
System Date	06-05-2014 09:58:59 AM
System Uptime	0d 00:06:43
BIOS Version	v1.00
Firmware Version	v2.50 2014-01-17
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	U01141010004
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	40-d8-55-1a-f0-3a
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
CPU Load (100ms, 1s, 10s)	27%, 23%, 23%
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Figure 2-1.1: System Information (For example, Vi3026. Other models are the same)

Parameter Description

Model name: The model name of this device.

System description: This tells what this device is. Here, it is “20-Port 10/100/1000Base-T + 4 TP/ (100/1G) SFP Combo + 2 (100/1G) SFP PoE+ L2 Plus Managed Switch”. 26 total ports.

Location: It is the location where this switch is put. User-defined.

Contact: For easy management and maintenance of the device, you may write down the contact person and their phone number in case you need any help or support. You can configure this parameter through the device’s user interface or SNMP.

Device name: The name of the switch. User-defined.

System Date: This how the system time of the switch. Its format is day of the week, month, date, hours: minutes: seconds, year.

System up time: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

BIOS version: The version of the BIOS in this switch.

Firmware version: The firmware version in this switch.

Hardware-Mechanical version: The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware. The one after the hyphen is the version of mechanical.

Serial number: The serial number is assigned by the Manufacture.

Host IP address: This is IP address of the switch.

Subnet Mask: This displays the IP subnet mask assigned to the device.

Gateway IP Address: This displays the default gateway IP address assigned to the device

Host MAC address: This is the Ethernet MAC address of the management agent in this switch.

Console Baudrate: This displays the baudrate of RJ-45(COM) port.

RAM size: The size of the RAM in this switch.

Flash size: The size of the flash memory in this switch.

CPU Load: This displays the load measured as averaged over the last 100ms, 1sec and 10 seconds intervals.

Bridge FDB size: This displays the bridge FDB size information.

Transmit Queue: This displays the device’s transmit hardware priority queue information.

Maximum Frame size: This displays the device’s maximum frame size information.

Note: In all cases, after entering and applying settings, select either Save Start (see page 268) if you want to save the configuration each time the switch is started or Save User (see page 269) if the you want the setting saved only for the Admin level log in.

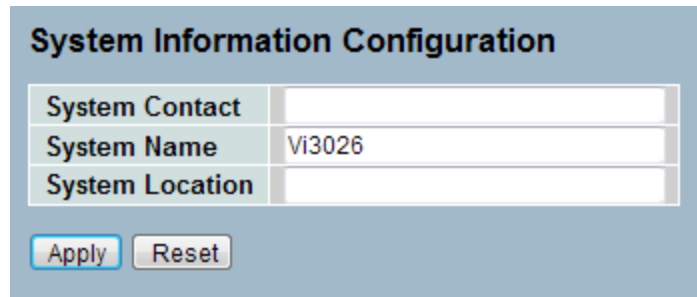
2-1.2 Configuration

You can identify the system by configuring the contact information, name, and location of the switch.

Web Interface

To configure System Information in the web interface:

1. Click System, System Information, then Configuration.
2. Write System Contact, System Name, System Location information on this page.
3. Click “Apply”.



System Information Configuration	
System Contact	<input type="text"/>
System Name	Vi3026
System Location	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 2-1.2: System Information Configuration

Parameter Description

System Contact: The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character cannot be a minus sign. The allowed string length is 0 to 255.

System Location: The physical location of this node (E.g. telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

2-2 Time

This page configures the switch's time. Time configure includes Time Configuration and NTP Configuration.

2-2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click Time, then Manual.
2. Specify the time parameter in manual parameters.
3. Click "Apply".

The screenshot displays the 'Time Configuration' web interface. It features a 'Clock Source' section with radio buttons for 'Use Local Settings' (selected) and 'Use NTP Server'. Below this is the 'Date and Time Format' section, showing a dropdown menu set to 'YYYY-MM-DD HH:MM:SS' and radio buttons for '24 hours' (selected) and '12 hours'. The 'Local Time' section contains input fields for Date (YYYY: 1999, MM: 12, DD: 31) and Time (HH: 8, MM: 2, SS: 34). The 'Time Zone Offset' is set to 480 min. The 'Daylight Savings' section has an 'Enable' checkbox. The 'Time Set Offset' is 60 min. The 'Daylight Savings Type' is set to 'By dates'. The 'From' and 'To' sections for the daylight savings period are empty, with input fields for Date (YYYY, MM, DD) and Time (HH, MM). At the bottom, there are 'Apply' and 'Reset' buttons, and a 'Time & Date' display showing '1999-12-31 08:02:34'.

Clock Source:	<input checked="" type="radio"/> Use Local Settings <input type="radio"/> Use NTP Server
Date and Time Format:	YYYY-MM-DD HH:MM:SS <input checked="" type="radio"/> 24 hours <input type="radio"/> 12 hours
Local Time:	Date YYYY: 1999 MM: 12 DD: 31 Time HH: 8 MM: 2 SS: 34
Time Zone Offset:	480 min
Daylight Savings:	<input type="checkbox"/> Enable
Time Set Offset:	60 min. (Range: 1 - 1440, Default: 60)
Daylight Savings Type:	<input checked="" type="radio"/> By dates <input type="radio"/> Recurring
From:	Date YYYY: MM: DD: Time HH: MM:
To:	Date YYYY: MM: DD: Time HH: MM:
From:	Day: Sun Week: First Month: Jan Time: HH: 0 MM: 0
To:	Day: Sun Week: First Month: Jan Time: HH: 0 MM: 0

Apply Reset

Time & Date
1999-12-31 08:02:34

Figure 2-2.1: The Time Configuration

Parameter Description

Clock Source: To view the Vi3026's clock source, select "Use local Settings" or "Use NTP Server".

Date and Time Format: The drop bar is for choose appropriate time format. Three selections are provided as below.

- YYYY-MM-DD HH:MM:SS
- MM-DD-YYYY HH:MM:SS
- DD-MM-YYYY HH:MM:SS
- 24 hours: The time is always represented in the 24-hour system
- 12 hours: The time is always represented in the 12-hour system

Local Time: Shows the current time of the system. The local time can only be set or filled out in 24 hours format.

Time Zone Offset: Provides the time zone offset relative to UTC/GMT. The benchmark based on GMT. The valid range is from -720 to 720 minutes

Daylight Saving: Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is -5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date. If you set daylight saving to be non-zero, you have to set the starting/ending date. Otherwise, the daylight saving function will not be activated.

Time Set Offset: Provides the daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. The default setting is 60 minutes. When using NTP, make sure the correct offset to GMT is used for your time zone.

Daylight Savings Type: Provides the Daylight savings type selection. You can select "By Dates" or "Recurring", two types for Daylight saving.

From: To configure when Daylight saving start date and time, the format is "YYYY-MM-DD HH:MM". The column "HH: MM" can only be set up in 24 hour format.

To: To configure when Daylight saving end date and time, the format is "YYYY-MM-DD HH:MM". The column "HH: MM" can only be set up in 24 hour format.



NOTE: The under "from" and "to" was displayed what you set on the "From" and "To" field information.



NOTE: The local time column and Day light saving column will not actively change by the date time format selection.

2-2.2 NTP

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing **<Apply>** button. Though, it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

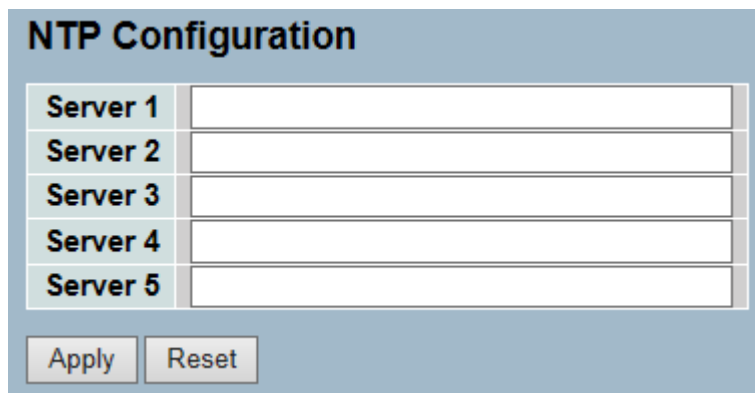
Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time. Otherwise, you will not able to get the correct time. The switch supports configurable time zone from -12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Web Interface

To configure Time in the web interface:

1. Click SYSTEM, then NTP.
2. Specify the Time parameter in manual parameters.
3. Click "Apply".



NTP Configuration	
Server 1	<input type="text"/>
Server 2	<input type="text"/>
Server 3	<input type="text"/>
Server 4	<input type="text"/>
Server 5	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 2-2.2: The NTP configuration

Parameter Description

Server 1 to 5: Provides the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

To confirm your connection to the NTP server, please ping the address you assign.

Buttons: These buttons are displayed on the NTP page -

- **Apply** – Click "Apply" to save changes.
- **Reset** - Click "Reset" to undo any changes made locally and revert back to previously saved values.

2-3 Account

In this function, only an administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password, but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

2-3.1 Users

This page provides an overview of the current users. Currently, the only way to login as another user on the web server is to close and reopen the browse.

Web Interface

To configure account in the web interface:

1. Click SYSTEM, Account, then Users.
2. Click "Add New User".
3. Specify the user name parameter.
4. Click "Apply".

The image shows two screenshots of a web interface. The top screenshot, titled "Users Configuration", displays a table with two columns: "User Name" and "Privilege Level". The table contains one entry: "admin" with a privilege level of "15". Below the table is a button labeled "Add new user", which is highlighted with a red rectangle. A red arrow points from this button to the bottom screenshot. The bottom screenshot, titled "Add User", shows a form for adding a new user. It has a section titled "User Settings" with four fields: "User Name", "Password", "Password (again)", and "Privilege Level". The "Privilege Level" field is a dropdown menu currently set to "1". At the bottom of the form are three buttons: "Apply", "Reset", and "Cancel".

User Name	Privilege Level
admin	15

Add new user

Add User

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	1 <input type="button" value="v"/>

Apply Reset Cancel

Figure 2- 3.1: The Users Account Configuration

**Parameter
Description**

User Name: The name identifying the user. This is also a link to add/edit User.

Password: To type the password. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Password (again): To type the password again. You must type the same password again in the field.

Privilege Level: The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups (e.g. that is granted the fully control of the device). But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. For system maintenance (software upload, factory defaults, and etc.), the user privilege needs to be level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

2-3.2 Privilege Level

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP MED, MAC Table, MRP, MVR, MVRP Maintenance, Mirroring, POE Ports, Private VLANs, QoS, SNMP, Security, Spanning Tree, System Trap Event, VCL, VLANs, and Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

1. Click SYSTEM, Account, then Privilege Level.
2. Specify the privilege parameter.
3. Click "Apply".

Group Name	Privilege Levels
Account	10
Aggregation	10
Diagnostics	10
EEE	10
Easyport	10
GARP	10
GVRP	10
IP	10
IPMC Snooping	10
LACP	10
LLDP	10
LLDP MED	10
Loop Protect	10
MAC Table	10
MVR	10
Maintenance	15
Mirroring	10
PoE	10
Ports	10
Private VLANs	10
QoS	10
SFlow	10
SNMP	10
Security	10
Single IP	10
Spanning Tree	10
System	10
Trap Event	10
UPnP	10
VCL	10
VLANs	10
Voice VLAN	10

Apply Reset

Figure 2- 3.2: The Privilege Level Configuration

Parameter Description

Group Name: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

- **System:** System Information, Time, Syslog.
- **Security:** IP Source Guard, ARP Inspection, DHCP snooping, DHCP Relay, NAS, Authentication (AAA), Port Security, System Access Management, ACL, HTTPS, SSH and Auth Method.
- **Account:** Users and Privilege Level.
- **Diagnostics:** Ping, Ping6 and VeriPHY.
- **Maintenance:** System Reboot, System Restore Default, Configuration Save, Export/Import Configuration and Firmware upgrade.

Privilege Levels: Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, and status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization privilege level to have the access to that group.

2-4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet Protocol is IPv4, which has 32-bits Internet Protocol addresses, allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

2-4.1 IPv4

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page:

- The "Configured" column is used to view or change the IP configuration.
- The "Current" column is used to show the active IP configuration.

Web Interface

To configure an IP address in the web interface:

1. Click System, then IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click "Apply".
4. To keep any changes through a power loss, be sure to save the "Start Configuration" as explained in section 5-3.2.

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	192.168.3.16	192.168.3.16
IP Mask	255.255.255.0	255.255.255.0
IP Gateway	192.168.3.254	192.168.3.254
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy ☐

Figure 2 - 4.1: The IP Configuration

**Parameter
Description**

DHCP Client: Enables the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IP Address: Provides the IP address of this switch in dotted decimal notation.

IP Mask: Provides the IP mask of this switch dotted decimal notation.

IP Gateway: Provides the IP address of the router in dotted decimal notation.

VLAN ID: Provides the managed VLAN ID. The allowed range is 1 to 4095.

DNS Server: Provides the IP address of the DNS Server in dotted decimal notation.

DNS Proxy: When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

2-4.2 IPv6

This section describes how to configure the switch-managed IPv6 information. The “Configured” column is used to view or change the IPv6 configuration. The “Current” column is used to show the active IPv6 configuration.

Configure the switch-managed IPv6 information on this page:

- The “Configured” column is used to view or change the IPv6 configuration.
- The “Current” column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the web interface:

1. Click System, then IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click “Apply”.
4. To keep any changes through a power loss, be sure to save the "Start Configuration" as explained in section 5-3.2.

IPv6 Configuration

	Configured	Current
Auto Configuration	<input type="checkbox"/>	<input type="button" value="Renew"/>
Address	<input type="text" value="::c0a8:0101"/>	<div><div>::c0a8:0101</div><div>Link-Local Address: fe80::0240:c7ff:fe12:3456</div></div>
Prefix	<input type="text" value="96"/>	96
Gateway	<input type="text" value="::"/>	::

Figure 2- 4.2: The IPv6 Configuration

Parameter Description

Auto Configuration: Enables IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address: Provides the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Prefix: Provides the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Gateway: Provides the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

2-5 Syslog

The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as a generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

2-5.1 Configuration

This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog configuration in the web interface:

1. Click SYSTEM, then Syslog.
2. Specify the syslog parameters include IP Address of Syslog server and Port number.
3. Evoke “Syslog” to enable it.
4. Click “Apply”.

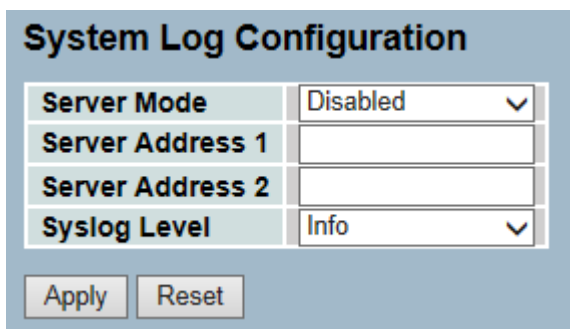


Figure 2- 5.1: The System Log Configuration

Parameter Description

Server Mode: Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

- **Enabled:** Enables server mode operation.
- **Disabled:** Disables server mode operation.

Server Address 1 and 2: Indicates the IPv4 host address of syslog server 1 and server 2 (For redundancy). If the switch provide DNS feature, it also can be a host name.

Syslog Level: Indicates what kind of message will send to syslog server. Possible modes are:

- <0> **Emergency:** System is unusable.
- <1> **Alert:** Action must be taken immediately.
- <2> **Critical:** Critical conditions.
- <3> **Error:** Error conditions.
- <4> **Warning:** Warning conditions.
- <5> **Notice:** Normal but significant conditions.
- <6> **Information:** Information messages.
- <7> **Debug:** Debug-level messages.

2-5.2 Log

This section describes how to display the system log information of the switch.

Web Interface

To display the log configuration in the web interface:

1. Click Syslog, then Log.
2. Display the log information.

ID	Level	Time	Message
1	Warning	2011-01-01 00:00:02	Switch just made a cold boot
2	Warning	2011-01-01 00:00:12	Link up on port 1
3	Info	2011-01-01 00:01:13	Login passed for user 'admin'
4	Info	2011-01-01 00:01:13	Login passed for user 'admin'

Figure 2- 5.2: The System Log configuration

Parameter Description

Auto-refresh: Click “Auto-Refresh” to refresh the log automatically.

ID: ID (≥ 1) of the system log entry.

Level: The level of the system log entry. The following level types are supported:

- <0> **Emergency:** System is unusable.
- <1> **Alert:** Action must be taken immediately.
- <2> **Critical:** Critical conditions.
- <3> **Error:** Error conditions.
- <4> **Warning:** Warning conditions.
- <5> **Notice:** Normal but significant conditions.
- <6> **Information:** Information messages.
- <7> **Debug:** Debug-level messages.

Time: It will display the log record by device time. The time of the system log entry.

Message: It will display the log detail message. The message of the system log entry.

Upper right icon (Refresh, clear...): You can click them to refresh the system log or clear them manually. Click other buttons to move to the next or previous pag.

2-5.3 Detailed Log

This section describes how to display the detailed log information of the switch.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Syslog, then Detailed Log.
2. Display the log information.

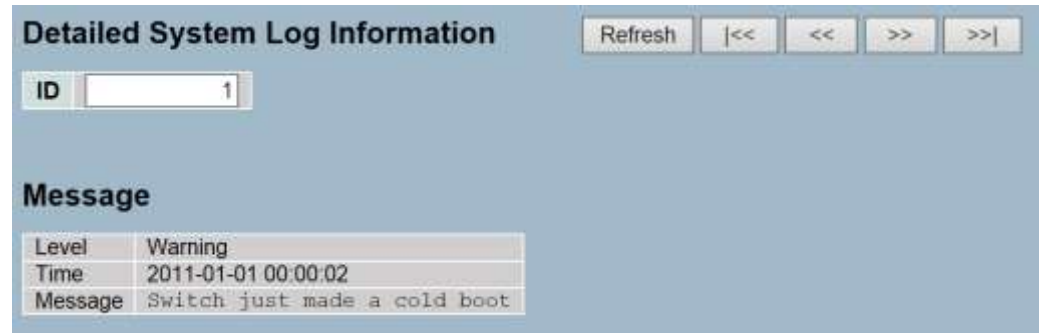


Figure 2-5.3: The Detailed System Log Information

Parameter Description

ID: The ID (≥ 1) of the system log entry.

Message: The detailed message of the system log entry.

Upper right icon (Refresh, clear,...): You can click them to refresh the system log or clear them manually. Click other buttons to move to the next or previous page.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

2-6.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps, as well as, the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. Both parties must have the same community name. Once the setting is completed, click **<Apply>** button so the setting can take effect.

Web Interface

To display the configure SNMP System in the web interface:

1. Click SNMP, then System.
2. Evoke “SNMP Stat”e to enable or disable the SNMP function.
3. Specify the “Engine ID”.
4. Click “Apply”.

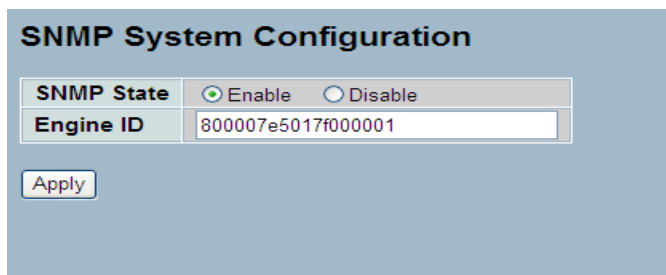
The image shows a web interface titled "SNMP System Configuration". It contains two main fields: "SNMP State" with radio buttons for "Enable" (selected) and "Disable", and "Engine ID" with a text input field containing the value "800007e5017f000001". Below these fields is an "Apply" button.

Figure 2- 6.1: The SNMP System Configuration

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

SNMP State: The term SNMP here is used for the activation or de-activation of SNMP.

Enable: Enables SNMP state operation.

Disable: Disables SNMP state operation.

Engine ID: SNMPv3 engine ID. syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet can't input 00. If the Engine ID changed, it will clear all original users.

2-6.2 Configuration

The function is used to configure SNMP communities. To enable a new community statistics, please check the button ▼, and choice **<Enable>** to configure SNMP function.

Web Interface

To display the configure SNMP Configuration in the web interface:

1. Click SNMP, then Configuration.
2. Evoke “SNMP State” to enable or disable the SNMP function.
3. Click “Apply”.

The image shows a web interface titled "SNMP Configuration". It contains two input fields: "Get Community" with the value "public__" and "Set Community" with the value "private". To the right of the "Set Community" field is a button labeled "Disable" and a dropdown arrow. Below these fields is an "Apply" button.

Figure 2- 6.2: The SNMP Configuration

Parameter Description

Get Community: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Set Community: Indicates the community writes access string to permit access to SNMP agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

2-6.3 Communities

The function is used to configure SNMPv3 communities. The Community and UserName are unique. To create a new community account, please check [<Add New Community>](#) button. Enter the account information and then check [<Save>](#).
Max Group Number: 4.

Web Interface

To display the configure SNMP Communities in the web interface:

1. Click SNMP, then Communities.
2. Click "Add New Community".
3. Specify the SNMP communities parameters.
4. Click "Apply".
5. If you want to modify or clear the setting, then click "Reset".

The screenshot displays the 'SNMPv1/v2 Communities to Security Configuration' web interface. It features a table with columns: Delete, Community, User Name, Source IP, and Source Mask. Below the table, there is a red-bordered button labeled 'Add new community' and an 'Apply' button. A red arrow points from the 'Add new community' button to the bottom section of the interface. The bottom section shows the same table with input fields for Community, User Name, Source IP (0.0.0.0), and Source Mask (0.0.0.0), along with 'Add new community' and 'Apply' buttons.

Figure 2- 6.2: The SNMPv1/v2 Communities Security Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Community: Indicates that the community access string permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

UserName: The UserName access string to permit access to SNMPv3 agent. The length of "UserName" string is restricted to 1-32.

Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: Indicates the SNMP access source address mask.

2-6.4 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check [Add New User](#) button. Enter the user information and then check [Save](#). Max Group Number: 10.

Web Interface

To display the configure SNMP Users in the web interface:

1. Click SNMP, then Users.
2. Specify the privilege parameter.
3. Click "Apply".

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	default_user	Auth, Priv	MD5	*****	DES	*****

[Add new user](#) [Apply](#)

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	<input type="text"/>	Auth, Priv	MD5	<input type="text"/>	DES	<input type="text"/>

[Add new user](#) [Apply](#)

Figure 2-6.3: The SNMP Users Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.
- The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- **None:** No authentication protocol.
- **MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.

Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- **None:** No privacy protocol.
- **DES:** An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password: A string of number identifies the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.5 Groups

The function is used to configure SNMPv3 group. The Entry index keys are Security Model and Security Name. To create a new group account, please check [Add new group](#) button. Enter the group information and then check [Save](#). Max Group Number: v1: 2, v2: 2, v3:10.

Web Interface

To display the configure SNMP Groups in the web interface:

1. Click SNMP, then Groups.
2. Specify the Privilege parameter.
3. Click "Apply".

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	usm	default_user	4

[Add new group](#) [Apply](#)

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Delete	usm	default_user	

[Add new group](#) [Apply](#)

Figure 2-6.4: The SNMP Groups Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- **V1:** Reserved for SNMPv1.
- **V2c:** Reserved for SNMPv2c.
- **Usm:** User-based Security Model (USM).

Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.6 Views

The function is used to configure SNMPv3 view. The entry index key is OID Subtree and View Name. To create a new view account, please check [<Add New View>](#) button, and enter the view information then check [<Save>](#). Max Group Number: 28.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

1. Click SNMP, then Views.
2. Click "Add New View".
3. Specify the SNMP view parameters.
4. Click "Apply".
5. If you want to modify or clear the setting then click "Reset".

The figure displays two screenshots of the 'SNMPv3 Views Configuration' web interface. The top screenshot shows the 'Add new view' button highlighted with a red box, with a red arrow pointing down to the bottom screenshot. The bottom screenshot shows the configuration form with the following fields: 'Delete' (a button), 'View Name' (a text input field), 'View Type' (a dropdown menu set to 'included'), and 'OID Subtree' (a text input field). Below these fields are 'Add new view' and 'Apply' buttons.

Figure 2-6.5: The SNMP Views Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type: Indicates the view type that this entry should belong to. Possible view types are:

- **Included:** An optional flag to indicate that this view subtree should be included.
- **Excluded:** An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

Apply: Click the "Save" icon save the configuration to ROM.

2-6.7 Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check [Add new access](#) button, and enter the access information then check [Save](#). Max Group Number: 14

Web Interface

To display the configure SNMP Access in the web interface:

1. Click SNMP, then Accesses.
2. Click "Add New Access".
3. Specify the SNMP access parameters.
4. Click "Apply".
5. If you want to modify or clear the setting, then click "Reset".

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	4	any	NoAuth, NoPriv	None	None
<input type="checkbox"/>	4	v1	NoAuth, NoPriv	None	None

[Add new access](#) [Apply](#)

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete	4	any	NoAuth, NoPriv	None	None

[Add new access](#) [Apply](#)

Figure 2-6.6: The SNMP Accesses Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- **Any:** Any security model accepted (v1|v2c|usm).
- **V1:** Reserved for SNMPv1.
- **V2c:** Reserved for SNMPv2c.
- **Usm:** User-based Security Model (USM).

Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

The name of the MIB view defines the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Button:

- **Add new access** - Click to add a new access entry.
- **Apply** - Click "Apply" to apply changes.

2-6.8 Trap

The function is used to configure SNMP trap. To create a new trap account, please check **<No number>** button and enter the trap information, then check **<Apply>**.
Max Group Number: 6.

Web Interface

To configure SNMP Trap setting:

1. Click SNMP, then Trap.
2. Display the SNMP Trap Hosts information table.
3. Choose an entry to display and modify the detail parameters, or click delete button to delete the trap hosts entry.

Trap Hosts Configuration

Delete No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
1								
2								
3								
4								
5								
6								

Apply

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Apply Reset

Figure 2-6.7: The SNMP Trap Host Configuration

Parameter
Description

Delete: Click [<Delete>](#) to delete the entry.

Trap Version: You may choose v1, v2c, or v3 trap.

Server IP: To assign the SNMP Host IP address.

UDP Port: To assign port number. Default: 162.

Community / Security Name: The length of “Community/Security Name” string is restricted to 1-32.

Severity Level: Indicates what kind of message will send to security level.

Possible modes are:

- **Info:** Send information, warnings, and errors.
- **Warning:** Send warnings and errors.
- **Error:** Send errors.

Security Level: There are three kinds of choices:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

Authentication Protocol: You can choose MD5 or SHA for authentication.

Authentication Password:

- The length of 'MD5 Authentication Password' is restricted to 8 – 32.
- The length of 'SHA Authentication Password' is restricted to 8 – 40.

Privacy Protocol: You can set DES encryption for UserName.

Privacy Password: The length of ' Privacy Password ' is restricted to 8 – 32.

Chapter 3: Configuration

3-1 Port

This chapter describes all of the basic network configuration tasks, which include the Ports, Layer 2 network protocol (e.g. VLANs, QoS, IGMP, ACLs, PoE, etc.) and any setting of the switch.

3-1.1 Configuration

The section describes how to configure the port detail parameters of the switch. You could use the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including:

- Linkup/Linkdown
- Speed (Current and configured)
- Flow Control (Current Rx, Current Tx, and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control.

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Configuration, Port, then Configuration
2. Specify the speed configured, flow control, maximum frame size, excessive collision mode and power control.
3. Click “Apply”.



NOTE: The flow control will be enabled only when the PD supports flow control function.

Port	Link	Current	Speed Configured	Current Rx	Current Tx	Configured	Maximum Frame Size	Excessive Collision Mode	Power Control
1	↑ Off	Down	Auto	×	×		9000	Discard	Disabled
2	↓	Down	Auto	×	×		9000	Discard	Disabled
3	↓	Down	Auto	×	×		9000	Discard	Disabled
4	↓	Down	Auto	×	×		9000	Discard	Disabled
5	↓	Down	Auto	×	×		9000	Discard	Disabled
6	↓	Down	Auto	×	×		9000	Discard	Disabled
7	↓	Down	Auto	×	×		9000	Discard	Disabled
8	↓	Down	Auto	×	×		9000	Discard	Disabled
9	↓	Down	Auto	×	×		9000	Discard	Disabled
10	↓	Down	Auto	×	×		9000	Discard	Disabled
11	↓	Down	Auto	×	×		9000	Discard	Disabled
12	↓	Down	Auto	×	×		9000	Discard	Disabled
13	↓	Down	Auto	×	×		9000	Discard	Disabled
14	↓	Down	Auto	×	×		9000	Discard	Disabled
15	↓	Down	Auto	×	×		9000	Discard	Disabled
16	↓	Down	Auto	×	×		9000	Discard	Disabled
17	↓	Down	Auto	×	×		9000	Discard	Disabled
18	↓	Down	Auto	×	×		9000	Discard	Disabled
19	↓	Down	Auto	×	×		9000	Discard	Disabled
20	↓	Down	Auto	×	×		9000	Discard	Disabled
21	↓	Down	SFP_Auto_AMS	×	×		9000	Discard	Disabled
22	↓	Down	SFP_Auto_AMS	×	×		9000	Discard	Disabled
23	↓	Down	SFP_Auto_AMS	×	×		9000	Discard	Disabled
24	↓	Down	SFP_Auto_AMS	×	×		9000	Discard	Disabled
25	↓	Down	Auto				9000		
26	↓	Down	Auto				9000		

Figure 3-1.1: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Link: The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed: Provides the current link speed of the port.

Configured Link Speed: Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:

- **Disabled** - Disables the switch port operation.
- **Auto** - Cu port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
- **10Mbps HDX** - Forces the cu port in 10Mbps half-duplex mode.
- **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode.
- **100Mbps HDX** - Forces the cu port in 100Mbps half-duplex mode.
- **100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode.
- **1Gbps FDX** - Forces the cu port in 1Gbps full duplex mode.
- **SFP_Auto_AMS** - Automatically determines the speed of the SFP. **Note:** There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode with SFP preferred. Cu port is set in **Auto** mode.
- 100-FX - SFP port in 100-FX speed. Cu port disabled.
- 100-FX_AMS - SFP port in 100-FX speed. Cu port disabled.
- 1000-X - SFP port in 1000-X speed. Cu port disabled.
- 1000-X_AMS - Port in AMS mode with SFP preferred. SFP port in 1000-X speed. Cu port in **Auto** mode.

LED Warning of Shared Cu ports Disabled:

Ports 21-24 are shared between the RJ45 connectors and SFP sockets. Whenever the left LED is blinking on any of these ports with no Rj45 cable inserted the RJ45 connector is disabled. To enable the Rj45 connector, using the GUI, navigate to Configuration,Port,Configuration and change the setting under "Speed Configured".

Flow Control (Auto mode will not read Flow Control): When “Auto Speed” is selected on a port. This section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The current Rx column indicates whether pause frames on the port are obeyed, and the current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last “Auto-Negotiation”.

Check The “Configured” column to use flow control. This setting is related to the setting for Configured Link Speed.

Maximum Frame Size: Enters the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode: Configures port transmit collision behavior.

- **Discard:** Discards frame after 16 collisions (default).
- **Restart:** Restarts back off algorithm after 16 collisions.

Power Control: The “Usage” column shows the current percentage of the power consumption per port. The “Configured” column allows for changing the power savings mode parameters per port.

- **Disabled:** All power savings mechanisms disabled.
- **ActiPHY:** Link down power savings enabled.
- **PerfectReach:** Link up power savings enabled.
- **Enabled:** Both link up and link down power savings enabled.

Buttons

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh): You can click them to refresh the port link status manually.

3-1.2 Port Description

The section describes how to configure the port's alias or any descriptions for the port Identity. It provides user to write down an alphanumeric string, describing the full name and version identification for the system's hardware type, software version, and networking application.

Web Interface

To configure a Port Description in the web interface:

1. Click Configuration, Port, then Port Description.
2. Specify the detail port alias or description an alphanumeric string, describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click "Apply".



Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	

Apply Reset

Figure 3-1.2: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Description: Enter up to 47 characters to be descriptive name for identifies this port.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset** - Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-1.3 Traffic Overview

The section describes how to the port statistics information and provides overview of general traffic statistics for all switch ports.

Web Interface

To display the Port Statistics Overview in the web interface:

- 1. Click Configuration, Port, then Traffic Overview
- 2. If you want to auto-refresh, select the “Auto-refresh” button.
- 3. Click “Refresh” to refresh the port statistics or clear all information when you click “Clear”.

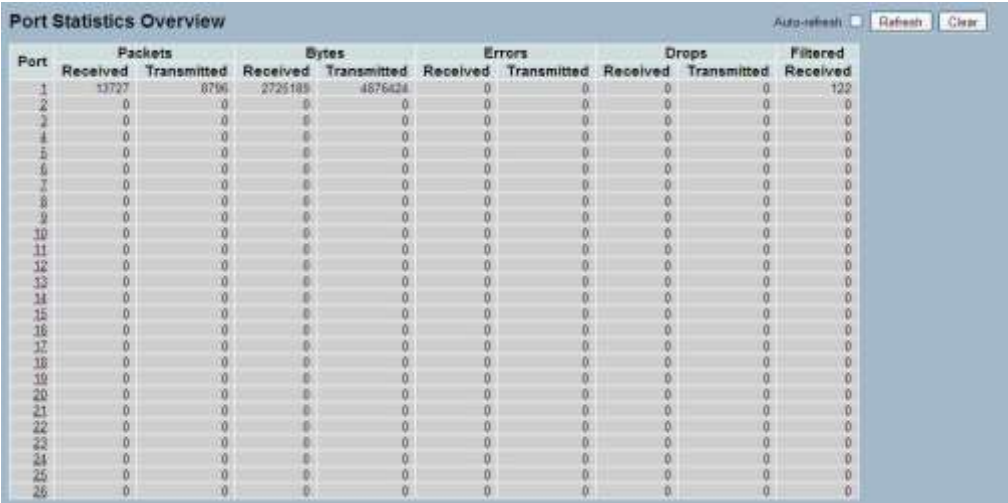


Figure 3-1.3: The Port Statistics Overview

Parameter Description

Port: The logical port for the settings contained in the same row.

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded due to ingress or egress congestion.

Filtered: The number of received frames filtered by the forwarding:

- **Auto-refresh:** Evoke the auto-refresh icon to refresh the information automatically.
- **Upper right icon (Refresh, Clear):** You can click them to refresh the port statistics information manually. Click “Clear” to clean up all port statistics.

3-1.4 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

- To display the Per Port detailed Statistics Overview in the web interface:
- 1. Click Configuration, Port, then Detailed Port Statistics.
 - 2. Scroll the “Port Index” to select which port you want to show the detailed port statistics overview”.
 - 3. If you want to auto-refresh the information, then select “Auto-refresh”.
 - 4. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

Detailed Port Statistics: Port 1				Port 1	Auto-refresh	Refresh	Clear
Receive Total		Transmit Total					
Rx Packets	3297	Tx Packets	2908				
Rx Octets	846974	Tx Octets	1412335				
Rx Unicast	3170	Tx Unicast	2388				
Rx Multicast	127	Tx Multicast	546				
Rx Broadcast	0	Tx Broadcast	3				
Rx Pause	0	Tx Pause	0				
Receive Size Counters		Transmit Size Counters					
Rx 64 Bytes	2047	Tx 64 Bytes	430				
Rx 65-127 Bytes	171	Tx 65-127 Bytes	65				
Rx 128-255 Bytes	83	Tx 128-255 Bytes	228				
Rx 256-511 Bytes	1022	Tx 256-511 Bytes	1390				
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	76				
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	791				
Rx 1527+ Bytes	0	Tx 1527+ Bytes	0				
Receive Queue Counters		Transmit Queue Counters					
Rx Q0	3297	Tx Q0	0				
Rx Q1	0	Tx Q1	0				
Rx Q2	0	Tx Q2	0				
Rx Q3	0	Tx Q3	0				
Rx Q4	0	Tx Q4	0				
Rx Q5	0	Tx Q5	0				
Rx Q6	0	Tx Q6	0				
Rx Q7	0	Tx Q7	2908				
Receive Error Counters		Transmit Error Counters					
Rx Drops	0	Tx Drops	0				
Rx CRC Alignment	0	Tx Late/Exp. Coll.	0				
Rx Undersize	0						
Rx Oversize	0						
Rx Fragments	0						
Rx Jabber	0						
Rx Filtered	124						

Figure 3-1.4: The Port Detail Statistics Overview

Parameter Description

- Auto-refresh:** Evoke the auto-refresh to refresh the port statistics information automatically.
- Upper left scroll bar:** To scroll which port to display the port statistics with “Port-0”, “Port-1” ...

Receive Total and Transmit Total

- Rx and Tx Packets:** The number of received and transmitted (good and bad) packets.
- Rx and Tx Octets:** The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
- Rx and Tx Unicast:** The number of received and transmitted (good and bad) unicast packets.
- Rx and Tx Multicast:** The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: The number of frames dropped due to the lack of receives buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames received with invalid CRC.

Rx Jabber: The number of long 2 frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

Auto-refresh: To evoke the auto-refresh to refresh the queuing counters automatically.

Upper right icon (Refresh, clear): You can click them to refresh the port detail statistics or clear them manually.

3-1.5 QoS Statistics

The section describes how to the switch could display the QoS detailed queuing counters for a specific switch port for the different queues for all switch ports.

Web Interface

To display the Queuing Counters in the web interface:

- 1. Click Configuration, Port, then QoS Statistics
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh the queuing counters or clear all information when you click " Clear".

Queuing Counters																		Auto-refresh <input type="checkbox"/>		Refresh	Clear
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7						
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx					
1	13929	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8929				
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				

Figure 3-1.5: The Queuing Counters Overview

Parameter Description

- Port:** The logical port for the settings contained in the same row.
- Qn:** Qn is the QoS queue number per port. Q0 is the lowest priority queue.
- Rx/Tx:** The number of received and transmitted packets per queue.
- Auto-refresh:** To evoke the auto-refresh to refresh the Queuing Counters automatically.
- Upper right icon (Refresh, clear):** You can click them to refresh the queuing counters or clear them manually.

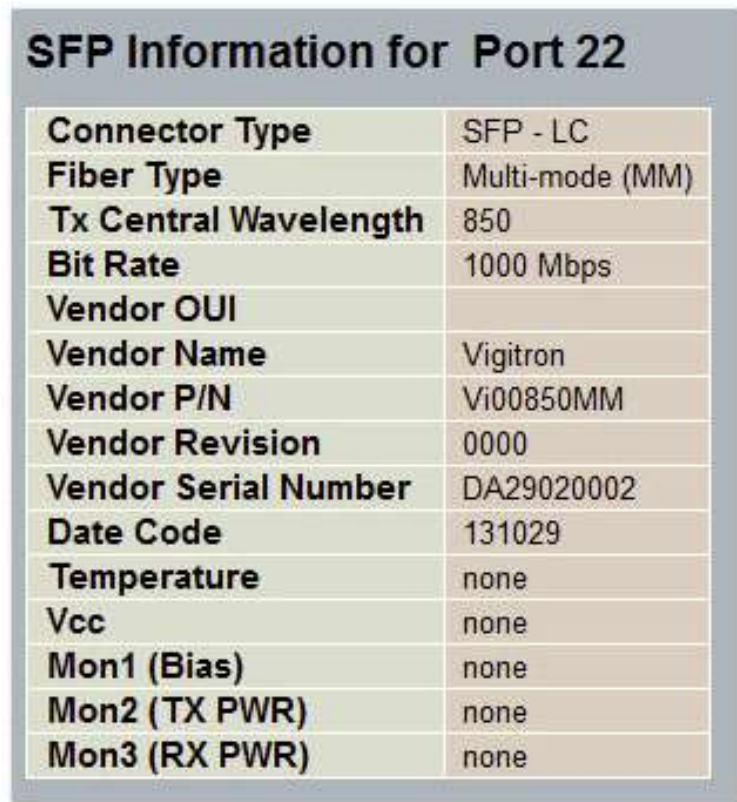
3-1.6 SFP Information

The section describes how to switch could display the SFP module detail information which you connect it to the switch. The information includes: connector type, fiber type, wavelength, baud rate, vendor OUI and more.

Web Interface

To display the SFP information in the web interface:

1. Click Configuration, Port, then SFP Information.
2. To display the SFP Information.



Connector Type	SFP - LC
Fiber Type	Multi-mode (MM)
Tx Central Wavelength	850
Bit Rate	1000 Mbps
Vendor OUI	
Vendor Name	Vigitron
Vendor P/N	Vi00850MM
Vendor Revision	0000
Vendor Serial Number	DA29020002
Date Code	131029
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figure 3-1.6: The SFP Information Overview

Parameter Description

Connector Type: Displays the connector type (e.g. UTP, SC, ST, LC and so on).

Fiber Type: Displays the fiber mode (e.g. Multi-Mode or Single-Mode).

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength (e.g. 850nm, 1310nm, 1550nm, and so on).

Baud Rate: Displays the maximum baud rate of the fiber module supported (e.g. 10M, 100M, 1G and so on).

Vendor OUI: Displays the manufacturer's OUI code which is assigned by IEEE.

Vendor Name: Displays the company name of the module manufacturer.

Vendor P/N: Displays the product name of the naming by module manufacturer.

Vendor Revision: Displays the module revision.

Vendor Serial Number: Shows the serial number assigned by the manufacturer.

Date Code: Shows the date this SFP module was made.

Temperature: Shows the current temperature of SFP module.

Vcc: Shows the working DC voltage of SFP module.

Mon1 (Bias) mA: Shows the Bias current of SFP module.

Mon2 (TX PWR): Shows the transmit power of SFP module.

Mon3 (RX PWR): Shows the receiver power of SFP module.



NOTE: Only SFP modules that are UL and CDRH Certified and have an international certification such as TUV, VDE, or DEMKO are recommended. Use only Class 1 SFP modules.

3-1.7 EEE

The section shows the user instructions on how to inspect and configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting devices have all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

For maximum power saving, the circuit doesn't start when data are ready to be transmitted. Instead, the circuit is queued until 3000 bytes of data are ready to be transmitted. To avoid a large delay in case that data less than 3000 bytes shall be transmitted, data are always transmitted after 48 us, to give a maximum latency of 48 us + the wakeup time.

If desired, it is possible to minimize the latency for specific frames by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE Configuration in the web interface:

1. Click Configuration, Port, then EEE.
2. To evoke which port wants to enable the EEE function.
3. Choose EEE Urgent Queues level and the range from 1 to 8. The queue will postpone the transmissions until 3000 bytes are ready to be transmitted.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Port	EEE Enabled	EEE Urgent Queues							
		1	2	3	4	5	6	7	8
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

Figure 3-1.7: The EEE Configuration

Parameter Description

EEE Port Configuration: The EEE port settings relate to the currently selected, as reflected by the page header.

Port: The switch port number of the logical EEE port.

EEE Enabled: Controls whether EEE is enabled for this switch port.

EEE Urgent Queues: Queues set will activate transmission of frames as soon as any data is available. Otherwise, the queue will postpone the transmission until 3000 bytes are ready to be transmitted.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**– Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-2 ACL

The Vi3026 switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes - IPv4, ARP protocol, MAC, and VLAN parameters. In this section, we will go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port. The policy number is 1-8. However, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3-2.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port, unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the web interface:

- 1. Click Configuration, ACL, then Ports.
- 2. Scroll the specific parameter value to select the correct value for port ACL setting.
- 3. Click "Apply" to save the setting.
- 4. If you want to cancel the setting, then you need to click the reset button to revert back to previously saved values.
- 5. After your configuration is complete, then you could see the counter of the port. You could click refresh to update the counter or clear the information.



Figure 3-2.1: The ACL Ports Configuration

Parameter Description

Port: The logical port for the settings contained in the same row.

Policy ID: Selects the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action: Selects whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID: Selects which rate limiter to apply on this port. The allowed values are "Disabled" or the values 1 through 16. The default value is "Disabled".

Port Redirect: Selects which port frames are redirected on. The allowed values are "Disabled" or a specific port number. The default value is "Disabled".

Mirror: Specifies the mirror operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

Logging: Specifies the logging operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are stored in the System Log.
- **Disabled:** Frames received on the port are not logged.
- The default value is "Disabled". Please note that the system log memory size and logging rate is limited.

Shutdown: Specifies the port shut down operation of this port. The allowed values are:

- **Enabled:** If a frame is received on the port, the port will be disabled.
- **Disabled:** Port shut down is disabled.
- The default value is "Disabled".

State: Specifies the port state of this port. The allowed values are:

- **Enabled:** To reopen ports by changing the volatile port configuration of the ACL user module.
- **Disabled:** To close ports by changing the volatile port configuration of the ACL user module.
- The default value is "Enabled".

Counter: Counts the number of frames that match this ACE.

Buttons:

- **Apply** – Click "Apply" to apply changes.
- **Reset** – Click "Reset" to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh, clear): You can click them to refresh the ACL Port Configuration or clear them manually.

3-2.2 Rate Limiters

The section describes how to configure the switch’s ACL rate limiter parameters. The rate limiter Level from 1 to 16 allows the user to set rate limiter value and units with pps or kbps.

Web Interface

- To configure ACL Rate Limiter in the web interface:
1. Click Configuration, ACL, then Rate Limiter.
 2. Specify the “Rate” field and the range from 0 to 3276700.
 3. To scroll the unit with pps or kbps.
 4. Click “Apply” to save the setting.
 5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*		<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

ApplyReset

Figure 3-2.2: The ACL Rate Limiter Configuration

Parameter
Description

Rate Limiter ID: The rate limiter ID for the settings contained in the same row.

Rate: The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, .., 1000000 in kbps.

Unit: Specify the rate unit. The allowed values are:

- **Pps:** Packets per second.
- **Kbps:** Kbits per second.

Buttons

- **Apply** – Click “Apply” to apply changes.
- **Reset** - Click “Reset” to undo any changes made locally and revert back to previously saved values.


3-2.3 Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permitted or denied conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted. The order sequence cannot be changed and the priority is highest.

Web Interface

To configure Access Control List in the web interface:

1. Click Configuration, ACL, then Configuration.
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (e.g. edit, delete, or moving the relative position of entry in the list).
3. To specific the parameter of the ACE.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.
6. When editing an entry on the ACE Configuration page, please note that the items displayed depend on various selections, such as frame type and IP protocol type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (e.g. Rate Limiter, Port Copy, Logging, and Shutdown).

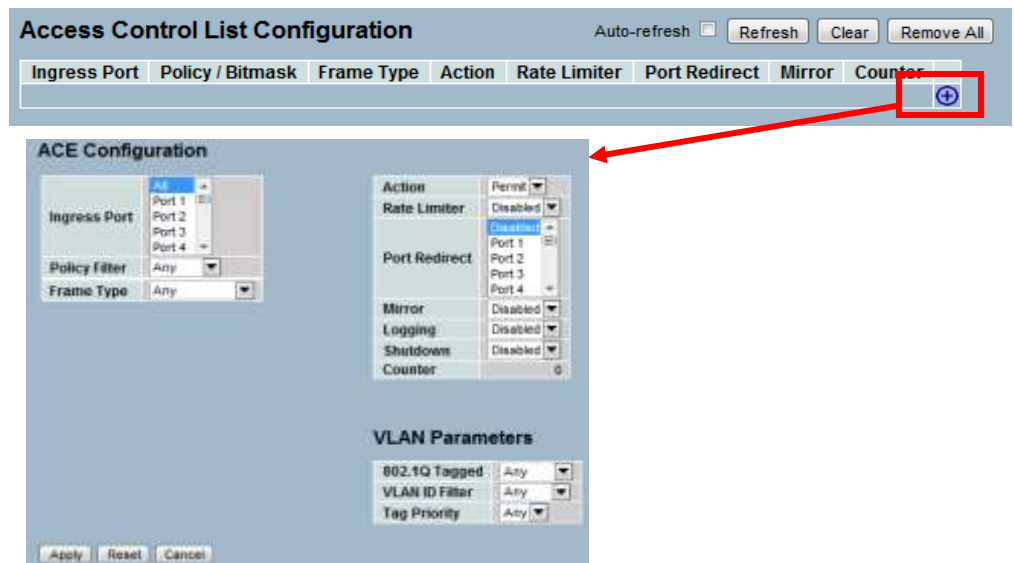


Figure 3-2.3: The ACL Rate Limiter Configuration

Parameter Description

Ingress Port: Select the ingress port for which this ACE applies.

- **All:** The ACE applies to all port.
- **Port n:** The ACE applies to this port number, where “n” is the number of the switch port.

Policy Filter: Specify the policy number filter for this ACE.

- **Any:** No policy filter is specified (policy filter status is "don't-care").
- **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.

Police Value: When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask: When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

Frame Type: Indicates the frame type of the ACE. Possible values are:

- **Any:** The ACE will match any frame type.
- **Ethernet type:** Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).
- **ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.
- **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.
- **IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action: Specify the action to take with a frame that hits this ACE.

- **Permit:** The frame that hits this ACE is granted permission for the ACE operation.
- **Deny:** The frame that hits this ACE is dropped.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When “Disabled” is displayed, the rate limiter operation is disabled.

Port Redirect: Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. “Disabled” indicates that the port redirect operation is disabled.

Mirror: Specifies the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

Logging: Indicates the logging operation of the ACE. Possible values are:

- **Enabled:** Frames matching the ACE are stored in the System Log.
- **Disabled:** Frames matching the ACE are not logged.
- Please note that the system log memory size and logging rate is limited.

Shutdown: Indicates the port shut down operation of the ACE. Possible values are:

- **Enabled:** If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

Counter: The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

SMAC Filter: *(Only displayed when the frame type is Ethernet Type or ARP)*
Specifies the source MAC filter for this ACE:

- **Any:** No SMAC filter is specified (SMAC filter status is "don't-care").
- **Specific:** If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value: When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx", "xx.xx.xx.xx.xx.xx", or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter: Specifies the destination MAC filter for this ACE.

- **Any:** No DMAC filter is specified (DMAC filter status is "don't-care").
- **MC:** Frame must be multicast.
- **BC:** Frame must be broadcast.
- **UC:** Frame must be unicast.
- **Specific:** If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

Counter: When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx", "xx.xx.xx.xx.xx.xx", or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged: Specifies whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

- **Any:** Any value is allowed ("don't-care").
- **Enabled:** Tagged frame only.
- **Disabled:** Untagged frame only.
- The default value is "Any".

VLAN ID Filter: Specifies the VLAN ID filter for this ACE.

- **Any:** No VLAN ID filter is specified (VLAN ID filter status is "don't-care").
- **Specific:** If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID: When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4094. A frame that hits this ACE matches this VLAN ID value.

Tag Priority: Specifies the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value "Any" means that no tag priority is specified (tag priority is "don't-care").

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP: Specifies the available ARP/RARP opcode (OP) flag for this ACE.

- **Any:** No ARP/RARP OP flag is specified (OP is "don't-care").
- **ARP:** Frame must have ARP/RARP opcode set to ARP.
- **RARP:** Frame must have ARP/RARP opcode set to RARP.
- **Other:** Frame has unknown ARP/RARP Opcode flag.

Request/Reply: Specifies the available ARP/RARP opcode (OP) flag for this ACE.

- **Any:** No ARP/RARP OP flag is specified (OP is "don't-care").
- **Request:** Frame must have ARP Request or RARP Request OP flag set.
- **Reply:** Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter: Specifies the sender IP filter for this ACE.

- **Any:** No sender IP filter is specified (sender IP filter is "don't-care").
- **Host:** Sender IP filter is set to "Host". Specifies the sender IP address in the SIP Address field that appears.
- **Network:** Sender IP filter is set to Network. Specifies the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address: When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask: When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter: Specifies the target IP filter for this specific ACE.

- **Any:** No target IP filter is specified (target IP filter is "don't-care").
- **Host:** Target IP filter is set to "Host". Specifies the target IP address in the Target IP Address field that appears.
- **Network:** Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address: When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask: When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP SMAC Match: Specifies whether frames can hit the action according to their sender hardware address field (SHA) settings.

- **0:** ARP frames where SHA is not equal to the SMAC address.
- **1:** ARP frames where SHA is equal to the SMAC address.
- **Any:** Any value is allowed ("don't-care").

RARP DMAC Match: Specifies whether frames can hit the action according to their target hardware address field (THA) settings.

- **0:** RARP frames where THA is not equal to the DMAC address.
- **1:** RARP frames where THA is equal to the DMAC address.
- **Any:** Any value is allowed ("don't-care").

IP/Ethernet Length: Specifies whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

- **0:** ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
- **1:** ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
- **Any:** Any value is allowed ("don't-care").

IP: Specifies whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

- **0:** ARP/RARP frames where the HLD is not equal to Ethernet (1).
- **1:** ARP/RARP frames where the HLD is equal to Ethernet (1).
- **Any:** Any value is allowed ("don't-care").

Ethernet: Specifies whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

- **0:** ARP/RARP frames where the PRO is not equal to IP (0x800).
- **1:** ARP/RARP frames where the PRO is equal to IP (0x800).
- **Any:** Any value is allowed ("don't-care").

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter: Specifies the IP protocol filter for this ACE.

- **Any:** No IP protocol filter is specified ("don't-care").
- **Specific:** If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
- **ICMP:** Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
- **UDP:** Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- **TCP:** Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value: When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL: Specifies the "Time-to-Live" settings for this ACE.

- **Zero:** IPv4 frames with a "Time-to-Live" field greater than zero must not be able to match this entry.
- **Non-zero:** IPv4 frames with a "Time-to-Live" field greater than zero must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

IP Fragment: Specifies the fragment offset settings for this ACE. This involves the settings for the “More Fragments” (MF) bit and the “Fragment Offset” (FRAG OFFSET) field for an IPv4 frame.

- **No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
- **Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

IP Option: Specifies the options flag setting for this ACE.

- **No:** IPv4 frames where the options flag is set must not be able to match this entry.
- **Yes:** IPv4 frames where the options flag is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

SIP Filter: Specifies the source IP filter for this ACE.

- **Any:** No source IP filter is specified (source IP filter is "don't-care").
- **Host:** Source IP filter is set to “Host”. Specifies the source IP address in the SIP Address field that appears.
- **Network:** Source IP filter is set to Network. Specifies the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address: When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask: When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter: Specifies the destination IP filter for this ACE.

- **Any:** No destination IP filter is specified (destination IP filter is "don't-care").
- **Host:** Destination IP filter is set to “Host”. Specifies the destination IP address in the DIP Address field that appears.
- **Network:** Destination IP filter is set to “Network”. Specifies the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address: When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask: When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

ICMP Parameter

ICMP Type Filter: Specifies the ICMP filter for this ACE.

- **Any:** No ICMP filter is specified (ICMP filter status is "don't-care").
- **Specific:** If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value: When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter: Specifies the ICMP code filter for this ACE.

- **Any:** No ICMP code filter is specified (ICMP code filter status is "don't-care").
- **Specific:** If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value: When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

TCP/UDP Source Filter: Specifies the TCP/UDP source filter for this ACE.

- **Any:** No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").
- **Specific:** If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
- **Range:** If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source NO.: When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range: When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter: Specifies the TCP/UDP destination filter for this ACE.

- **Any:** No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
- **Specific:** If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
- **Range:** If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number: When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range: When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN: Specifies the TCP "No more data from sender" (FIN) value for this ACE.

- **0:** TCP frames where the FIN field is set must not be able to match this entry.
- **1:** TCP frames where the FIN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP SYN: Specifies the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

- **0:** TCP frames where the SYN field is set must not be able to match this entry.
- **1:** TCP frames where the SYN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP RST: Specifies the TCP "Reset the connection" (RST) value for this ACE.

- **0:** TCP frames where the RST field is set must not be able to match this entry.
- **1:** TCP frames where the RST field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP PSH: Specifies the TCP "Push Function" (PSH) value for this ACE.

- **0:** TCP frames where the PSH field is set must not be able to match this entry.
- **1:** TCP frames where the PSH field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP ACK: Specifies the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- **0:** TCP frames where the ACK field is set must not be able to match this entry.
- **1:** TCP frames where the ACK field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP URG: Specifies the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- **0:** TCP frames where the URG field is set must not be able to match this entry.
- **1:** TCP frames where the URG field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

IP Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

Ether Type Filter: Specifies the Ethernet type filter for this ACE.

- **Any:** No EtherType filter is specified (EtherType filter status is "don't-care").
- **Specific:** If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value: When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP), and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Modification Buttons: You can modify each ACE (Access Control Entry) in the table using the following buttons:



: Inserts a new ACE before the current row.



: Edits the ACE row.



: Moves the ACE up the list.



: Moves the ACE down the list.



: Deletes the ACE.



: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons:

- **Apply** – Click “Apply” to apply changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

Auto-refresh: Click “Auto-refresh” to refresh the information automatically.

Upper right icon (Refresh, clear, Remove All): You can click them to refresh the ACL configuration or clear them manually. Click other buttons to remove all ACL configurations on the table.

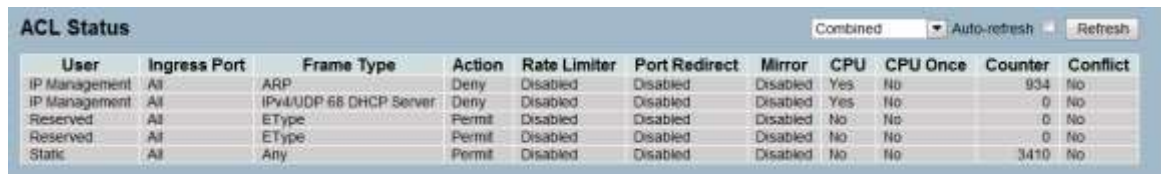
3-2.4 ACL Status

The section describes how to show the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Configuration, ACL, then ACL status.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the ACL Status.



The screenshot shows the 'ACL Status' web interface. At the top, there is a dropdown menu set to 'Combined', an 'Auto-refresh' button, and a 'Refresh' button. Below this is a table with the following columns: User, Ingress Port, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, CPU, CPU Once, Counter, and Conflict. The table contains five rows of data:

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	934	No
IP Management	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Static	All	Any	Permit	Disabled	Disabled	Disabled	No	No	3410	No

Figure 3-2.4: The ACL Rate Limiter Configuration

Parameter Description

User: Indicates the ACL user.

Ingress Port: Indicates the ingress port of the ACE. Possible values are:

- **All:** The ACE will match all ingress port.
- **Port:** The ACE will match a specific ingress port.

Frame Type: Indicates the frame type of the ACE. Possible values are:

- **Any:** The ACE will match any frame type.
- **EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
- **ARP:** The ACE will match ARP/RARP frames.
- **IPv4:** The ACE will match all IPv4 frames.
- **IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.
- **IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.
- **IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.
- **IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
- **IPv6:** The ACE will match all IPv6 standard frames.

Action: Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When "Disabled" is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are "Disabled" or a specific port number. When "Disabled" is displayed, the port redirect operation is disabled.

Mirror: Specifies the mirror operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

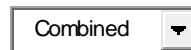
CPU: Forward packet that matched the specific ACE to CPU.

CPU Once: Forward first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Auto-refresh: Evoke "Auto-refresh" to refresh the information automatically.



: Selects the ACL status from this drop down list.

Upper right icon (Refresh): You can click them to refresh the ACL status information manually.

3-3 Aggregation

Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full-duplex and the same MAC to be a single logical port. Thus, the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment’s to build the bandwidth aggregation. For example, if there are three fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single fast Ethernet port has.

3-3.1 Static Trunk

The Aggregation configuration is used to configure the settings of “Link Aggregation”. You can bundle more than one port with the same speed, full-duplex and the same MAC to be a single logical port. Thus, the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment’s to build the bandwidth aggregation.

3-3.1.1 Static Trunk

Ports using “Static Trunk” as their trunk method can choose their unique Static GroupID to form a logic “trunked port”. The benefit of using “Static Trunk” method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using “Static Trunk” on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

- 1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
- 2. Evoke to enable or disable the aggregation mode function. Evoke Aggregation Group ID and Port members.
- 3. Click “Apply” to save the setting.
- 4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

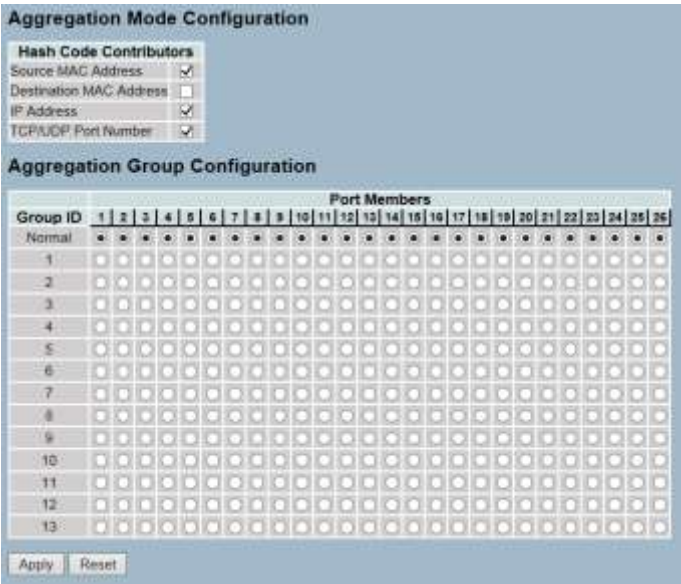


Figure 3-3.1.1: The Aggregation Mode Configuration

Parameter Description

Hash Code Contributors

Source MAC Address: The source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the source MAC address or uncheck to disable. By default, the source MAC Address is enabled.

Destination MAC Address: The destination MAC address can be used to calculate the destination port for the frame. Check to enable the use of the destination MAC address or uncheck to disable. By default, the destination MAC address is disabled.

IP Address: The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP address or uncheck to disable. By default, IP address is enabled.

TCP/UDP Port Number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number or uncheck to disable. By default, the TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID: Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full-duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset** – Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

3-3.2.1 Configuration

This section allows the user to inspect and change the current LACP port configurations. A LACP trunk group with more than one ready member-ports is a “real trunked” group. A LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, then Configuration.
2. Evoke to enable or disable the LACP on the port of the switch. Scroll the Key parameter with Auto or Specific Default is Auto.
3. Scroll the Role with Active or Passive. The default is “Active”.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Port	LACP Enabled	Key	Role
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Auto	Active
2	<input type="checkbox"/>	Auto	Active
3	<input type="checkbox"/>	Auto	Active
4	<input type="checkbox"/>	Auto	Active
5	<input type="checkbox"/>	Auto	Active
6	<input type="checkbox"/>	Auto	Active
7	<input type="checkbox"/>	Auto	Active
8	<input type="checkbox"/>	Auto	Active
9	<input type="checkbox"/>	Auto	Active
10	<input type="checkbox"/>	Auto	Active
11	<input type="checkbox"/>	Auto	Active
12	<input type="checkbox"/>	Auto	Active
13	<input type="checkbox"/>	Auto	Active
14	<input type="checkbox"/>	Auto	Active
15	<input type="checkbox"/>	Auto	Active
16	<input type="checkbox"/>	Auto	Active
17	<input type="checkbox"/>	Auto	Active
18	<input type="checkbox"/>	Auto	Active
19	<input type="checkbox"/>	Auto	Active
20	<input type="checkbox"/>	Auto	Active
21	<input type="checkbox"/>	Auto	Active
22	<input type="checkbox"/>	Auto	Active
23	<input type="checkbox"/>	Auto	Active
24	<input type="checkbox"/>	Auto	Active
25	<input type="checkbox"/>	Auto	Active
26	<input type="checkbox"/>	Auto	Active

Apply Reset

Figure 3-3.2.1: The LACP Port Configuration

**Parameter
Description**

Port: The switch port number.

LACP Enabled: Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs.

Key: The key value incurred by the port, ranging from 1-65535 . The “Auto” setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the “Specific” setting, a user-defined value can be entered. Ports with the same key value can participate in the same aggregation group, while ports with different keys cannot.

Role: The “Role” shows the LACP activity status. “Active” will transmit LACP packets each second, while “Passive” will wait for a LACP packet from a partner (speak if spoken to).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-3.2.2 System Status

This section describes how to set up the LACP function on the switch, then it provides a status overview for all LACP instances

Web Interface

To display the LACP System status in the web interface:

- 1. Click Configuration, LACP, then System Status.
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh the LACP System Status.



Figure 3-3.2.2: The LACP System Status

Parameter Description

Aggr ID: The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID: The system ID (MAC address) of the aggregation partner.

Partner Key: The Key that the partner has assigned to this aggregation ID.

Last changed: The time since this aggregation changed.

Local Ports: Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Auto-refresh: Evoke "Auto-refresh" to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the LACP System status information manually.

3-3.2.3 Port Status

This section describes how to set up the LACP function on the switch, then it provides a Port Status overview for all LACP instances.

Web Interface

To display the LACP Port status in the web interface:

- 1. Click Configuration, LACP, then Port Status.
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh the LACP Port Status.

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No				
2	No				
3	No				
4	No				
5	No				
6	No				
7	No				
8	No				
9	No				
10	No				
11	No				
12	No				
13	No				
14	No				
15	No				
16	No				
17	No				
18	No				
19	No				
20	No				
21	No				
22	No				
23	No				
24	No				
25	No				
26	No				

Figure 3-3.2.3: The LACP Status

Parameter Description

- Port:** The port number of the switch.
- LACP:** 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile, the LACP status is disabled.
- Key:** The key assigned to this port. Only ports with the same key can aggregate together.
- Aggr ID:** The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
- Partner System ID:** The partner's system ID (MAC address).
- Partner Port:** The partner's port number connected to this port.
- Auto-refresh:** Evoke "Auto-refresh" to refresh the information automatically.
- Upper right icon (Refresh):** You can click them to refresh the LACP port status information manually.

3-3.2.4 Port Statistics

This section describes how to set up the LACP function on the switch in order to provide a port statistics overview for all LACP instances.

Web Interface

- To display the LACP Port status in the web interface:
- 1. Click Configuration, LACP, then Port Statistics.
 - 2. If you want to auto-refresh the information, then you need to evoke the “Auto refresh”.
 - 3. Click “Refresh” to refresh the LACP Statistics.

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

Figure 3-3.2.4: The LACP Statistics

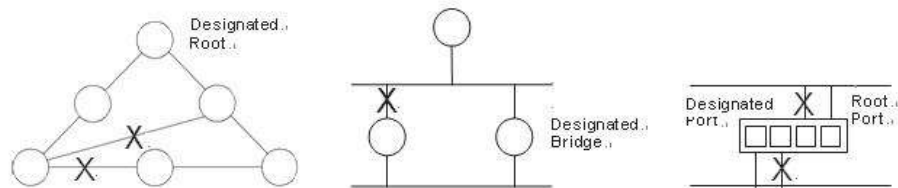
Parameter Description

- Port:** The switch port number.
- LACP Received:** Shows how many LACP frames have been received at each port.
- LACP Transmitted:** Shows how many LACP frames have been sent from each port.
- Discarded:** Shows how many unknown or illegal LACP frames have been discarded at each port.
- Auto-refresh:** Evoke “Auto-refresh” to refresh the information automatically.
- Upper right icon (Refresh, Clear):** You can click them to refresh the LACP port statistics information or clear manually.

3-4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. It also provides backup links, which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge, or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device), which incurs the lowest path cost when forwarding a packet from that device to the root device. Then, it selects a designated bridging device from each LAN, which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3-4.1 Bridge Settings

The section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings used by all STP Bridge instance in the switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, then Bridge Settings.
2. Scroll to select the parameters and write down available value of parameter in blank field in "Basic Settings".
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in advanced settings.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

The screenshot shows the 'STP Bridge Configuration' window. It has two main sections: 'Basic Settings' and 'Advanced Settings'. The 'Basic Settings' section contains a table with the following values: Protocol Version (MSTP), Bridge Priority (32768), Forward Delay (15), Max Age (20), Maximum Hop Count (20), and Transmit Hold Count (6). The 'Advanced Settings' section contains four checkboxes: Edge Port BPDU Filtering, Edge Port BPDU Guard, Port Error Recovery, and Port Error Recovery Timeout, all of which are currently unchecked. At the bottom of the window are 'Apply' and 'Reset' buttons.

Basic Settings	
Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Apply Reset

Figure 3-4.1: The STP Bridge Configuration

Parameter Description

Basic Settings

Protocol Version: The STP protocol version setting. Valid values are STP, RSTP, and MSTP.

Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age: The maximum age of the information transmitted by the bridge when it is the root bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count: This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering: Controls whether a port explicitly configured as "Edge" will transmit and receive BPDUs.

Edge Port BPDU Guard: Controls whether a port explicitly configured as "Edge" will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery: Controls whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, the ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

2-4.2 MSTI Mapping

When you implement a Spanning Tree protocol on the switch, the CIST is not available for explicit mapping because it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (e.g. not having any VLANs mapped to it.)

This section allows the user to inspect and change the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, then MSTI Mapping.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click “Apply” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

MSTI Configuration

Add VLANs separated by spaces or comma.
Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name: 00-40-c7-12-34-56
Configuration Revision: 0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Apply Reset

Figure 3-4.2: The MSTI Configuration

Parameter Description

Configuration Identification

Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as, the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI: The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (e.g. not having any VLANs).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-4.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch, the CIST is the default instance which is always active. For controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a bridge identifier.

The section describes it allows the user to inspect and change the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, then MSTI Priorities.
2. Scroll the Priority maximum is 240. The default is 128.
3. Click “Save” to apply the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

The screenshot shows the 'MSTI Configuration' web interface. It features a table titled 'MSTI Priority Configuration' with two columns: 'MSTI' and 'Priority'. The table lists instances from CIST to MSTI7, all with a priority of 32768. Below the table are 'Apply' and 'Reset' buttons.

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Figure 3-4.3: The MSTI Configuration

Parameter Description

MSTI: The bridge instance. The CIST is the default instance, which is always active.

Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset** – Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance, you need to configure the CIST Ports. The section allows the user to inspect and change the current STP CIST port configurations.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, then CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scroll and evoke to set all parameters of the CIST normal Port configuration.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	BPDU Guard	Portfast
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
11	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
12	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
13	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
14	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
15	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
16	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
17	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
18	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
19	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
20	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
21	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
22	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
23	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
24	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
25	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast
26	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Portfast

Apply Reset

Figure 3-4.4: The STP CIST Port Configuration

Parameter
Description

Port: The switch port number of the logical STP port.

STP Enabled: Controls whether STP is enabled on this switch port.

Path Cost: Controls the path cost incurred by the port. The auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200,000,000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

AdminEdge: Controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).

AutoEdge: Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from, whether BPDU's are received on the port or not.

Restricted Role: If enabled, it causes the port not to be selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as "Root Guard".

Restricted TCN: If enabled, it causes the port not to propagate received topology change notifications and topology changes to other ports. It can also cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard: If enabled, it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge port error recovery setting as well.

Point to Point: Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**– Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-4.5 MSTI Ports

The section allows the user to inspect and change the current STP MSTI port configurations.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, then MSTI Ports.
2. Scroll to select the “MST1” or other MSTI Port.
3. Click “Set” to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI port configuration.
5. Click “Apply” to save the setting.
6. If you want to cancel the setting, click the reset button to revert back to previously saved values.

MSTI Port Configuration

Select

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
Auto		128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128
13	Auto	128
14	Auto	128
15	Auto	128
16	Auto	128
17	Auto	128
18	Auto	128
19	Auto	128
20	Auto	128
21	Auto	128
22	Auto	128
23	Auto	128
24	Auto	128
25	Auto	128
26	Auto	128
27	Auto	128
28	Auto	128

Figure 3-4.5: The MSTI Port Configuration

**Parameter
Description**

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: Controls the path cost incurred by the port. The “Auto” setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the “Specific” setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-4.6 Bridge Status

After you complete the MSTI port configuration that you could to ask the switch display the bridge status. The section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Configuration, Spanning Tree, then STP Bridges.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00:00:40:C7:12:34:56	80:00:00:40:C7:12:34:56	-	0	Steady	-

Figure 3-4.6: The STP Bridges status

Parameter Description

MSTI: MSTI is the bridge instance. It's also a link to the STP detailed bridge status.

Bridge ID: The bridge ID of this bridge instance.

Root ID: The bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: It's the root path cost. It is zero for the root bridge. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Topology Flag: The current state of the topology flag change of this bridge instance.

Topology Change Last: The time since last topology change occurred.

Auto-refresh: Evoke auto-refresh to refresh the information automatically.

Upper right icon (Refresh): You can click the icon to refresh the STP bridges status information manually.

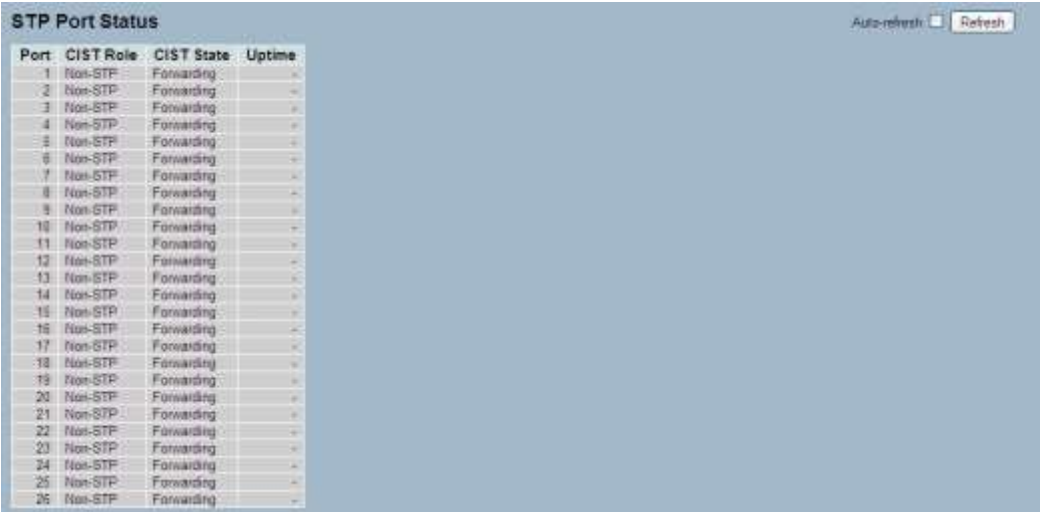
3-4.7 Port Status

After you complete the STP configuration, you could ask the switch to display the STP port status. This section allows you to ask the switch to display the STP CIST port status for all physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

- 1. Click Configuration, Spanning Tree, then STP Port Status.
- 2. If you want to auto-refresh the information, click “Auto-refresh”.
- 3. Click “Refresh” to refresh the STP Bridges.



The screenshot shows the 'STP Port Status' web interface. It features a table with four columns: Port, CIST Role, CIST State, and Uptime. The table lists 26 ports, all of which are in the 'Forwarding' state. In the top right corner, there is an 'Auto-refresh' checkbox (which is unchecked) and a 'Refresh' button.

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-

Figure 3-4.7: The STP Port status

Parameter
Description

- Port:** The switch port number of the logical STP port.
- CIST Role:** The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, or DesignatedPort Disabled.
- CIST State:** The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, or Forwarding.
- Uptime:** The time since the bridge port was last initialized.
- Auto-refresh:** Evoke “Auto-refresh” to refresh the information automatically.
- Upper right icon (Refresh):** You can click the icon to refresh the STP Port status information manually.

3-4.8 Port Statistics

After you complete the STP configuration, then you could let the switch display the STP Statistics. The section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

- 1. Click Configuration, Spanning Tree, then Port Statistics.
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh the STP Bridges.

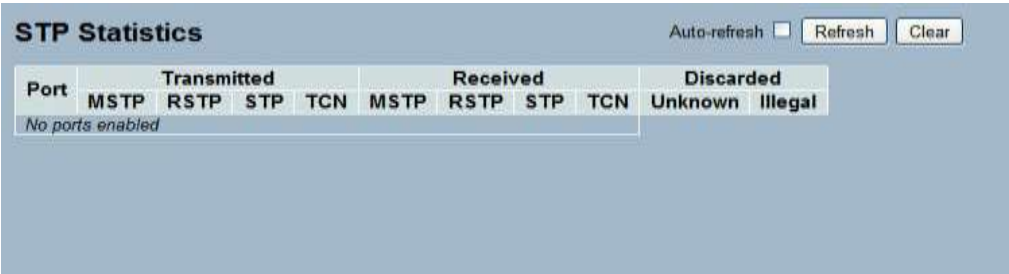


Figure 3-4.8: The STP Statistics

Parameter Description

- Port:** The switch port number of the logical STP port.
- MSTP:** The number of MSTP Configuration BPDU's received/transmitted on the port.
- RSTP:** The number of RSTP Configuration BPDU's received/transmitted on the port.
- STP:** The number of legacy STP Configuration BPDU's received/transmitted on the port.
- TCN:** The number of (legacy) "Topology Change Notification" BPDU's received/transmitted on the port.
- Discarded Unknown:** The number of unknown spanning tree BPDU's received (and discarded) on the port.
- Discarded Illegal:** The number of illegal spanning tree BPDU's received (and discarded) on the port.
- Auto-refresh:** Evoke "Auto-refresh" to refresh the information automatically.
- Upper right icon (Refresh, Clear):** You can click them to refresh the STP statistics information or clear manually.

3-5 IGMP Snooping

The function is used to establish the multicast groups to forward the multicast packet to the member ports, and in nature, to avoid wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch that supports IGMP Snooping with the functions of query, report and leave (a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host) can update the information of the Multicast table when a member (port) joins or leaves an IP multicast destination address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built in advance. The IGMP mode enables the switch to issue IGMP functions (IGMP proxy or snooping) on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3-5.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, then Basic Configuration.
2. Evoke to enable or disable a specific global configuration.
3. Evoke which port you want to become a Router Port, or enable/disable the Fast Leave function.
4. Scroll to set the throttling parameter.
5. Click "Apply" to save the setting.
6. If you want to cancel the setting, click the reset button to revert back to previously saved values.

IGMP Snooping Configuration			
Global Configuration			
Snooping Enabled		<input type="checkbox"/>	
Unregistered IPMCv4 Flooding Enabled		<input type="checkbox"/>	
IGMP SSM Range		232.0.0.0 / 8	
Proxy Enabled		<input type="checkbox"/>	
Port Related Configuration			
Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Apply Reset

Figure 3-5.1: The IGMP Snooping Configuration.

Parameter Description

Snooping Enabled: Enables the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled: Enables unregistered IPMCv4 traffic flooding.

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask).

Proxy Enabled: Enables IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: It shows the physical port index of switch.

Router Port: Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enables the fast leave on the port.

Throttling: Enables to limit the number of multicast groups to which a switch port can belong.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-5.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP snooping function. Each setting page shows up to 99 entries from the VLAN table. The default is 20 and can be selected through the "Entries Per Page" input field. During your first visit, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. By clicking the button, the displayed table will update, starting from that or the next closest VLAN table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

- 1. Click Configuration, IGMP Snooping, then VLAN Configuration.
- 2. Evoke to enable or disable Snooping IGMP Querier. Specify the parameters in the blank field.
- 3. Click "Refresh" to update the data or click "<< or >>" to display previous entry or next entry.
- 4. Click "Apply" to save the setting.
- 5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

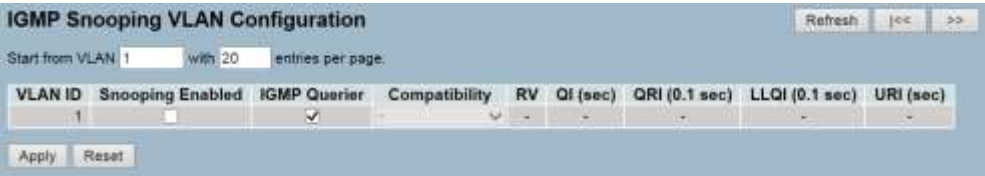


Figure 3-5.2: The IGMP Snooping VLAN Configuration.

Parameter Description

- VLAN ID:** It displays the VLAN ID of the entry.
- Snooping Enabled:** Enables the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
- IGMP Querier:** A router sends IGMP query messages onto a particular link. This router is called the "Querier". Enables the IGMP querier in the VLAN.
- Compatibility:** Compatibility is maintained by hosts and routers taking appropriate actions, depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, or Forced IGMPv3. The default compatibility value is "IGMP-Auto".
- RV:** Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.
- QI:** Query Interval. The query interval is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.
- QRI:** Query Response Interval. The max response time used to calculate the "Max Resp Code" inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Last Member Query Interval. The last member query time is the time value represented by the last member query interval, multiplied by the last member query count. The allowed range is 0 to 31744 in tenths of seconds. The default last member query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The unsolicited report interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds. The default unsolicited report interval is 1 second.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**– Click “Reset” to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh, |<<, >>): You can click the icon to refresh the displayed table starting from the "VLAN" input fields. Or click “|<<” to update the table starting from the first entry in the VLAN table (e.g. the entry with the lowest VLAN ID). Click “>>” to update the table, starting with the entry after the last entry currently displayed.

3-5.3 Port Group Filtering

The section describes how to set the “IGMP Port Group Filtering”. With the IGMP filtering feature, a user can exert this type of control. In some network application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IGMP Snooping, then Port Group Filtering.
2. Click “Add New Filtering Group”.
3. Scroll the port to enable the “Port Group Filtering”. Specify the “Filtering Groups” in the blank field.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

IGMP Snooping Port Group Filtering Configuration

Delete Port Filtering Groups

Add new Filtering Group

Apply Reset

IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Delete	14 ▼	
Delete	11 ▼	
Delete	1 ▼	

Add new Filtering Group

Apply Reset

Figure 3-5.3: The IGMP Snooping Port Group Filtering Configuration.

**Parameter
Description**

Delete: Check to delete the entry. It will be deleted during the next save.

Port: To evoke the port enable the IGMP Snooping Port Group Filtering function.

Filtering Groups: The IP multicast group that will be filtered.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-5.4 Status

After you complete the IGMP snooping configuration, then you could let the switch display the IGMP snooping status. The section describes how to let the switch display the IGMP snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Configuration, IGMP Snooping, Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Status.
4. Click “Clear” to clear the IGMP Snooping Status.

IGMP Snooping Status Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-

Figure 3-5.4: The IGMP Snooping Status.

**Parameter
Description**

VLAN ID: The VLAN ID of the entry.

Querier Version: Working querier version currently.

Host Version: Working host version currently.

Querier Status: Shows the querier status is "ACTIVE" or "IDLE".

Queries Transmitted: The number of transmitted queries.

Queries Received: The number of received queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Port: Switch port number.

Status: Indicate whether specific port is a router port or not.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, clear): You can click them to refresh the status or clear them manually.

3-5.5 Group Information

After you set the IGMP snooping function, then you could let the switch to display the IGMP snooping group information. Entries in the IGMP group table are shown on this page. The IGMP group table is sorted first by VLAN ID and then by group. The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No More Entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

- 1. Click Configuration, IGMP Snooping, then Group Information.
- 2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh the entry of the IGMP Snooping Groups Information.
- 4. Click "<< or >>" to move to previous or next entry.



Figure 3-5.5: The IGMP Snooping Groups Information.

Parameter Description

Navigating the IGMP Group Table

The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the IGMP Group Table. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No More Entries" is shown in the displayed table.

IGMP Group Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): You can click them to refresh the IGMP Group Status manually. Click "<<" or ">>" to move to the next or previous page.

3-5.6 IPv4 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host indicates that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the web interface:

1. Click Configuration, IGMP Snooping, then IPv4 SSM Information.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh an entry of the IGMPv3 IPv4 SSM Information.
4. Click "<< or >>" to move to previous or next entry.



Figure 3-6.6: The IGMPv3 IPv4 SSM Information.

Parameter Description

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information table. The default is 20, selected through the "Entries Per Page" input field. During the first visit, the web page will show the first 20 entries from the beginning of the IGMPv3 Information Table.

The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMPv3 information table match. In addition, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address upon a button click.

This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No More Entries" is shown in the displayed table. Use the buttons to start over.

IGMPv3 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, Port Number, Group Address) basis. It can be either "Include" or "Exclude".

Source Address: IP address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the type. It can be either "Allow" or "Deny".

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

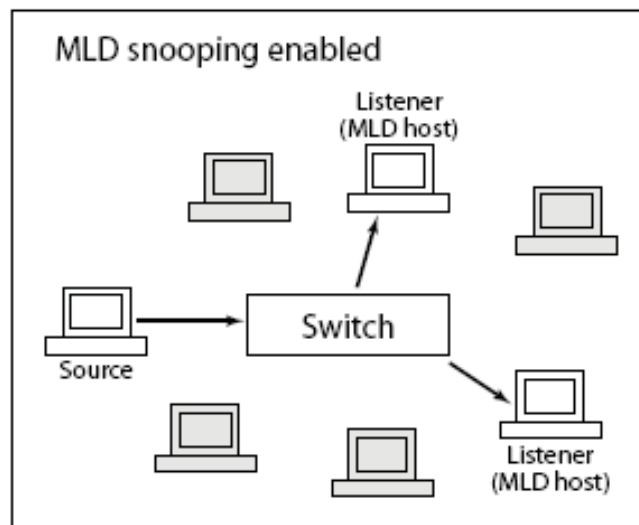
Upper right icon (Refresh, <<, >>): You can click them to refresh the IGMP group status manually. Click "<<" or ">>" to move to the next or previous page.

3-6 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping. It just provides multicast traffic and MLD doesn't interact with it. **Note:** In an application like desktop conferencing a network node may act as both a source and an MLD host. However, MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. **Note:** This is a function of the application software, not of MLD.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



3-6.1 Basic Configuration

The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, MLD Snooping, then Basic Configuration.
2. Evoke to enable or disable the global configuration parameters. Evoke the port to join router port and fast leave.
3. Scroll to select the throttling mode with "Unlimited" or 1 to 10.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

MLD Snooping Configuration

Global Configuration

Snooping Enabled ☐

Unregistered IPMCv6 Flooding Enabled ☐

MLD SSM Range: / 96

Proxy Enabled ☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Apply Reset

Figure 3-6.1: The MLD Snooping Basic Configuration.

Parameter Description

Snooping Enabled: Enables the global MLD snooping.

Unregistered IPMCv6 Flooding Enabled: Enables unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of “Neighbor Discovery”.

MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (using IPv6 address) range.

Proxy Enabled: Enables MLD proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: The port index what you enable or disable the MLD snooping function.

Router Port: Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Evokes to enable the fast leave on the port.

Throttling: Enables to limit the number of multicast groups to which a switch port can belong.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-6.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

It will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "No More Entries" is shown in the displayed table. Use the buttons to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

- 1. Click Configuration, MLD Snooping, then VLAN Configuration.
- 2. Specify the VLAN ID with entries per page.
- 3. Click "Refresh" to refresh an entry of the MLD Snooping VLAN Configuration Information.
- 4. Click "<< or >>" to move to previous or next entry.



Figure 3-7.2: The MLD Snooping VLAN Configuration.

Parameter Description

VLAN ID: The VLAN ID of the entry.

Snooping Enabled: Enables the per-VLAN MLD snooping. Only up to 32 VLANs can be selected.

MLD Querier: A router sends MLD query messages onto a particular link. This router is called the "Querier". It enables the MLD querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, and Forced MLDv2. The default compatibility value is "MLD-Auto".

Rv: Robustness Variable. The robustness variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.

QI: Query Interval. The query interval is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.

QRI: Query Response Interval. The maximum response delay used to calculate the maximum response code inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Last Listener Query Interval. The last listener query interval is the maximum response delay used to calculate the maximum response code inserted into multicast address specific queries sent in response to version 1 multicast listener done messages. It is also the maximum response delay used to calculate the maximum response code inserted into multicast address and source specific query messages. The allowed range is 0 to 31744 in tenths of seconds. The default last listener query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The unsolicited report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds. The default unsolicited report interval is 1 second.

Upper right icon (Refresh, <<, >>): You can click them to refresh the IGMP group status manually. Click "<<" or ">>" to move to the next or previous page.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-6.3 Port Group Filtering

The section describes how to you could to set the port group filtering in the mld snooping function. On the UI, you could add new filtering group and safety policy.

Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, MLD Snooping, then Port Group Filtering Configuration.
2. Click “Add New Filtering Group”.
3. Specify the filtering groups with entries per page.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

The figure shows two screenshots of the MLD Snooping Port Group Filtering Configuration web interface. The top screenshot shows the 'Add new Filtering Group' button highlighted with a red box and a red arrow pointing to the bottom screenshot. The bottom screenshot shows the configuration table with columns 'Delete', 'Port', and 'Filtering Groups'. The 'Port' column has a dropdown menu showing '1'. The 'Filtering Groups' column is empty. Below the table are buttons for 'Add new Filtering Group', 'Apply', and 'Reset'.

Figure 3-7.3: The MLD Snooping Port Group Filtering Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings. You can evoke to enable the port to join filtering Group

Filtering Groups: The IP Multicast Group that will be filtered.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-6.4 Status

The section describes when you complete the MLD snooping, and how To display the MLD snooping status and detail information. It will help you to find out the detail information of MLD snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

- 1. Click Configuration, MLD Snooping, then Status.
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh an entry of the MLD snooping status Information.
- 4. Click "Clear" to clear the MLD snooping status.



Figure 3-6.4: The MLD Snooping Status

Parameter Description

- VLAN ID :** The VLAN ID of the entry.
- Querier Version:** Working querier version currently.
- Host Version:** Working host version currently.
- Querier Status:** Show the querier status is "ACTIVE" or "IDLE".
- Queries Transmitted:** The number of transmitted queries.
- Queries Received:** The number of received queries.
- V1 Reports Received:** The number of Received V1 Reports.
- V2 Reports Received:** The number of Received V2 Reports.

V1 Leaves Received: The number of Received V1 Leaves.

Auto-refresh: Evoke “Auto-refresh” to refresh the log automatically.

Upper right icon (Refresh, <<, >>): You can click them to refresh the IGMP Group Status manually. Click “<<” or “>>” to move to the next or previous page.

3-6.5 Group Information

The section describes how the user could set the MLD snooping groups Information. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLD group table.

Each page shows up to 99 entries from the MLD group table. The default is 20 and can be selected through the "Entries Per Page" input field. During the first visit, the web page will show the first 20 entries from the beginning of the MLD Group Table.

Web Interface

To display the MLD Snooping Group information in the web interface:

- 1. Click Configuration, MLD Snooping, then Group Information.
- 2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh an entry of the MLD Snooping Group Information.
- 4. Click "Clear" to clear the MLD Snooping Groups information.



Figure 3-6.5: The MLD Snooping Groups Information

Parameter Description

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD group table. The default is 20 and can be selected through the "Entries Per Page" input field. During the first visit, the web page will show the first 20 entries from the beginning of the MLD group table. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLD group table. Clicking the button will update the displayed table starting from that or the next closest.

MLD group table match. In addition, the two input fields will assume the value of the first displayed entry upon a button click. This allows for continuous refresh with the same start address. It will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached, the text "No More Entries" is shown in the displayed table. Use the button to start over.

MLD Snooping Information Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): You can click them to refresh the IGMP Group Status manually. Click "<< or >>" to move to the next or previous page.

3-6.6 IPv6 SSM
Information

The section describes how the user can configure the entries in the MLDv2 information table are shown on this page. The MLDv2 information table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information table. The default is 20 and can be selected through the "Entries Per Page" input field. During the first visit, the web page will show the first 20 entries from the beginning of the MLDv2 information table. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLDv2 information table.

Web Interface

To display the MLDv2 IPv6 SSM information in the web interface:

- 1. Click Configuration, MLD Snooping, then IPv6 SSM Information.
- 2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
- 3. Click "Refresh" to refresh an entry of the MLDv2 IPv6 SSM Information.
- 4. Click "<< or >>" to move to previous or next entry.



Figure 3-6.6: The IPv6 SSM Information

Parameter
description

MLDv2 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either "Include" or "Exclude".

Source Address: IP address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the type. It can be either "Allow" or "Deny".

3-7 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to switch A so it can join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

3-7.1 Configuration

The section describes how the user could set the MVR basic configuration and some parameters in the switch.

Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

- 1. Click Configuration, MVR, Configuration2. Scroll the MVR mode to enable or disable ,and to set all parameters.
- 2. Click “Apply” to save the setting.
- 3. If you want to cancel the setting, click the reset button to revert back to previously saved values.

MVR Configuration

MVR Mode

Disabled

VLAN ID

100

Port Configuration

Port	Mode	Type	Immediate Leave
*	<div></div>	<div></div>	<div></div>
1	Disabled	Receiver	Disabled
2	Disabled	Receiver	Disabled
3	Disabled	Receiver	Disabled
4	Disabled	Receiver	Disabled
5	Disabled	Receiver	Disabled
6	Disabled	Receiver	Disabled
7	Disabled	Receiver	Disabled
8	Disabled	Receiver	Disabled
9	Disabled	Receiver	Disabled
10	Disabled	Receiver	Disabled
11	Disabled	Receiver	Disabled
12	Disabled	Receiver	Disabled
13	Disabled	Receiver	Disabled
14	Disabled	Receiver	Disabled
15	Disabled	Receiver	Disabled
16	Disabled	Receiver	Disabled
17	Disabled	Receiver	Disabled
18	Disabled	Receiver	Disabled
19	Disabled	Receiver	Disabled
20	Disabled	Receiver	Disabled
21	Disabled	Receiver	Disabled
22	Disabled	Receiver	Disabled
23	Disabled	Receiver	Disabled
24	Disabled	Receiver	Disabled
25	Disabled	Receiver	Disabled
26	Disabled	Receiver	Disabled

Apply

Reset

Figure 3-7.1: The MVR Configuration

**Parameter
Description**

MVR Mode: Enables/Disables the Global MVR.

VLAN ID: Specifies the multicast VLAN ID.

Mode: Enables MVR on the port.

Type: Specifies the MVR port type on the port.

Immediate Leave: Enables the fast leave on the port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-7.2 Port Group Allow

The section describes how the user could add the IP Multicast Group, which allowed to receive the multicast stream. Entries in the MVR port group allow table is shown on this page. The MVR Port Group Table is sorted first by port, and then by IP address

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Configuration, MVR, then Port Groups Allow.
2. If you want to add the new allowed group, you need to click the “Add New Allow Group” button.
3. Evoke the “Port No.”, “Start Address”, and “End Address”.
4. To click the “Apply” to apply the configuration of MVR port group allow table.

The top screenshot shows the 'MVR Port Group Allow Configuration' interface. It features a table with headers: 'Delete', 'Port', 'Start Address', and 'End Address'. Below the table is a button labeled 'Add new Allow Group', which is highlighted with a red box. At the bottom are 'Apply' and 'Reset' buttons.

The bottom screenshot shows the same interface after clicking 'Add new Allow Group'. The table now contains one entry with 'Delete' (a button), 'Port' (a dropdown menu showing '1'), 'Start Address' (an empty text box), and 'End Address' (an empty text box). The 'Add new Allow Group' button is still present below the table.

Figure 3-7.2: The MVR Groups Information

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next apply.

Port: The logical port for the settings.

Allow Groups: The IP multicast group that will be allowed.

- **Adding New Allow Group:** Click “Add New Allow Group” to add a new entry to the group allow table. Specify the port and allow group of the new entry. Click “Apply”.
- **Buttons:**
 - Apply** – Click “Apply” to save changes.
 - Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-7.3 Groups Information

The section describes how the user could display the MVR groups detail information on the switch. Entries in the MVR group table are shown on this page. The MVR group table is sorted first by VLAN ID, and then by group.

Web Interface

To display the MVR Groups Information in the web interface:

- 1. Click Configuration, MVR, then Groups Information.
- 2. If you want to auto-refresh the information, then you need to evoke the “Auto-refresh”.
- 3. Click the “Refresh” to refresh an entry of the MVR Groups Information.
- 4. Click “<< or >>” to move to previous or next entry.



Figure 3-7.2: The MVR Groups Information

Parameter Description

MVR Group Table Columns

- VLAN ID:** VLAN ID of the group.
- Groups:** Group ID of the group displayed.
- Port Members:** Ports under this group.
- Auto-refresh:** Evoke “Auto-refresh” to refresh the information automatically.
- Upper right icon (Refresh, <<, >>):** You can click them to refresh the MVR Group information manually. Click “<< or >>” to move to the next or previous page.

3-7.4 Statistics

The section describes how the switch will display the MVR detail statistics after you had configured MVR on the switch. It provides the detail MVR statistics information.

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Configuration, MVR, then Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh".
1. Click the "Refresh" to refresh an entry of the MVR Statistics Information.
3. Click "<< or >>" to move to previous or next entry.



Auto-refresh <input type="checkbox"/> Refresh Clear				
VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Figure 3-7.3: The MVR Statistics Information

Parameter

Description

VLAN ID: The Multicast VLAN ID.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, <<, >>): You can click them to refresh the MVR Group information manually. Click "<< or >>" to move to the next or previous page.

3-8 LLDP

The switch supports the LLDP. For current information on your switch model, the “Link Layer Discovery Protocol” (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The “Link Layer Discovery Protocol” (LLDP) is a vendor-neutral link layer protocol in the internet protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as station and media access control connectivity discovery specified in standards document IEEE 802.1AB.

3-8.1 LLDP Configuration

You can do the LLDP configuration and the detail parameters per port. The settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click LLDP configuration.
2. Modify LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click “Apply”.

LLDP Configuration

LLDP Parameters

Tx Interval: 30 seconds

Tx Hold: 4 times

Tx Delay: 2 seconds

Tx Reinit: 2 seconds

Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Reset

Figure 3-8.1: The LLDP Configuration

Parameter Description

LLDP Parameters

Tx Interval: The switch periodically transmits LLDP frames to its neighbors to have the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold: Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx hold multiplied by Tx interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay: If some configuration is changed (e.g. the IP address), a new LLDP frame is transmitted. The time between the LLDP frames will always be at least the value of Tx delay seconds. Tx delay cannot be larger than 1/4 of the Tx interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit: When a port is disabled (LLDP is disabled or the switch is rebooted), a LLDP shutdown frame is transmitted to the neighboring units to signal that the LLDP information isn't valid anymore. Tx reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected, as reflected by the page header.

Port: The switch port number of the logical LLDP port.

Mode: Select LLDP mode.

- **Rx Only:** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
- **Tx Only:** The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- **Disabled:** The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- **Enabled:** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware: Select CDP awareness.

- The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.
- Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.
- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

- Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.
- If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.



NOTE: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets when the hold time is exceeded.

Port Descr: Optional TLV: When checked, the "port description" is included in LLDP information transmitted.

Sys Name: Optional TLV: When checked, the "system name" is included in LLDP information transmitted.

Sys Descr: Optional TLV: When checked, the "system description" is included in LLDP information transmitted.

Sys Capa: Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.

Mgmt Addr: Optional TLV: When checked, the "management address" is included in LLDP information transmitted.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

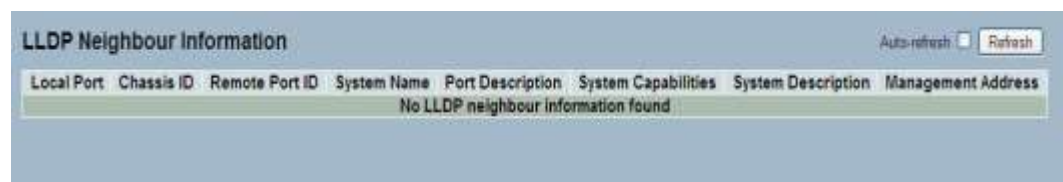
3-8.2 LLDP Neighbours

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected.

Web Interface

To show LLDP neighbours:

1. Click "LLDP Neighbours".
2. Click "Refresh" for manual update web screen.
3. Click "Auto-refresh" for auto-update web screen.



Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	System Description	Management Address
No LLDP neighbour information found							

Figure 3-8.2: The LLDP Neighbors information



NOTE: If your network without any device supports LLDP, then the table will show "No LLDP neighbour information found".

Parameter Description

Local Port: The port on which the LLDP frame was received.

Chassis ID: The chassis ID is the identification of the neighbour's LLDP frames.

Remote Port ID: The remote port ID is the identification of the neighbour port.

System Name: System name is the name advertised by the neighbour unit.

Port Description: Port description is the port description advertised by the neighbour unit.

System Capabilities: System capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

System Description: System description is the port description advertised by the neighbour unit.

Management Address: Management address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could hold the neighbour's IP address.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the LLDP neighbours information manually.

3-8.3 LLDP-MED Configuration

Media endpoint discovery is an enhancement of LLDP, known as LLDP-MED that provides the following facilities:

- Auto-discovery of LAN policies (e.g. VLAN, Layer 2 Priority and Differentiated services [Diffserv] settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and in the case of Voice over Internet Protocol (VoIP), enhanced 911 services.
- Extended and automated power management of power over Ethernet (PoE) end points.
- Inventory management allows network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click “LLDP-MED Configuration”.
2. Modify fast start repeat count parameter. The default is 4.
3. Modify “Coordinates Location” parameters.
4. Fill “Civic Address Location” parameters.
5. Add new policy.
6. Click “Apply” to show the policy port configuration.
7. Select policy ID for each port.
8. Click “Apply”.

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count: 4

Coordinates Location

Latitude: 0 degree North Longitude: 0 degree East Altitude: 0 Meters Map Datum: WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service:

Policies

Add new policy

Policy Port Configuration

Apply Reset

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Add new policy

Figure 3-8.3: The LLDP-MED Configuration

Parameter description

Fast start repeat count

Rapid startup and emergency call service location identification discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information, which are specifically relevant to particular endpoint type. For example, only advertise the voice network policy to permitted voice-capable devices. This conserves the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind, LLDP-MED defines an LLDP-MED fast start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a network connectivity device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED endpoint device is detected, will an LLDP-MED capable network connectivity device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With fast start repeat count, it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED fast start mechanism is only intended to run on links between LLDP-MED network connectivity devices and endpoint devices, and as such does not apply to links between LAN infrastructure elements, including network connectivity devices or other types of links.

Coordinates Location

Latitude: Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either north of the equator or south of the equator.

Longitude: Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either east of the prime meridian or west of the prime meridian.

Altitude: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

- **Meters:** Represents meters of altitude defined by the vertical datum specified.
- **Floors:** Represents altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum: The map datum is used for the coordinates given in these options:

- **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
- **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
- **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture).

County: County, parish, gun (Japan), district.

City: City, township, shi (Japan) - Example: Copenhagen.

City district: City division, borough, city district, ward, chou (Japan).

Block (Neighbourhood): Neighbourhood, block.

Street: Street - Example: Poppelvej.

Leading street direction: Leading street direction - Example: N.

Trailing street suffix: Trailing street suffix - Example: SW.

Street suffix: Street suffix - Example: Ave, Platz.

House no.: House number - Example: 21.

House no. suffix: House number suffix - Example: A, 1/2.

Landmark: Landmark or vanity address - Example: Columbia University.

Additional location info: Additional location info - Example: South Wing.

Name: Name (residence and office occupant) - Example: Flemming Jahn.

Zip code: Postal/zip code - Example: 2791.

Building: Building (structure) - Example: Low Library.

Apartment: Unit (Apartment, suite) - Example: Apt 42.

Floor: Floor - Example: 4.

Room no.: Room number - Example: 450F.

Place type: Place type - Example: Office.

Postal community name: Postal community name - Example: Leonia.

P.O. Box: Post office box (P.O. BOX) - Example: 12345.

Additional code: Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network policy discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements (e.g. interactive voice and/or video services).

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control/Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same network connectivity device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between network connectivity devices and endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Tag: Tag indicate whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as, the DSCP value. The tagged format includes an additional field known as the “Tag Header”. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP: DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy: Click to add a new policy. Specify the application type, tag, VLAN ID, L2 priority and DSCP for the new policy. Click "Save".

Port Policies Configuration:

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port: The port number to which the configuration applies.

Policy Id: The set of policies shall apply to a given port. The set of policies is selected by marking the checkboxes that corresponds to the policies.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-8.4 LLDP-MED Neighbours

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To show LLDP-MED neighbor:

1. Click "LLDP-MED Neighbor".
2. Click "Refresh" to manually update the web screen.
3. Click "Auto-refresh" to auto update the web screen.



Figure 3-9.4: The LLDP-MED Neighbours information



NOTE: If your network without any device supports LLDP-MED, then the table will show "No LLDP-MED Neighbour Information Found".

Parameter Description

Port: The port on which the LLDP frame was received.

Device Type:

- LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices.
- LLDP-MED network connectivity device definition.
- LLDP-MED network connectivity devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. An LLDP-MED network connectivity device is a LAN access device based on any of the following technologies:
 1. LAN Switch/Router
 2. IEEE 802.1 Bridge
 3. IEEE 802.3 Repeater (included for historical reasons)
 4. IEEE 802.11 Wireless Access Point
 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition: LLDP-MED endpoint devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED endpoint device category, the LLDP-MED scheme is broken into further endpoint device classes, as defined in the following.

Each LLDP-MED endpoint device class is defined to build upon the capabilities defined for the previous endpoint device class. For example, any LLDP-MED endpoint device claiming compliance as a media endpoint (Class II) also support all aspects of TIA-1057 applicable to generic endpoints (Class I), and any LLDP-MED endpoint device claiming compliance as a communication device (Class III) will also support all aspects of TIA-1057 applicable to both media endpoints (Class II) and generic endpoints (Class I).

LLDP-MED Generic Endpoint (Class I): The LLDP-MED generic endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057. However, it does not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP communication controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II): The LLDP-MED media endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous generic endpoint class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) voice/media gateways, conference bridges, media servers, and similar.

Discovery services defined in this class includes media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III): The LLDP-MED communication endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous generic endpoint (Class I) and media endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management.

LLDP-MED Capabilities: LLDP-MED capabilities describe the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type: Application Type indicates the primary function of the application(s) defined for this network policy, advertised by an endpoint or network connectivity device. The possible application types are shown below.

1. **Voice** - For use by dedicated IP telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signaling** - For use in network topologies that require a different policy for the voice signaling than for the voice media.
3. **Guest Voice** - Supports a separate limited feature-set voice service for guest-users and visitors with their own IP telephony handsets and other

similar appliances supporting interactive voice services.

4. **Guest Voice Signaling** - For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
5. **Softphone Voice** - For use by softphone applications on typical data centric devices, such as PCs or laptops.
6. **Video Conferencing** - For use by dedicated video conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - For use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. **Video Signaling** - For use in network topologies that require a separate policy for the video signaling than for the video media.

Policy: Policy indicates that an endpoint device wants to explicitly advertise that the policy is required by the device. It can be either “Defined” or “Unknown”.

- **Unknown:** The network policy for the specified application type is currently unknown.
- **Defined:** The network policy is defined.

TAG: TAG is an indication of whether the specified application type is using a tagged or an untagged VLAN. It can be “Tagged” or “Untagged”.

- **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
- **Tagged:** The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

3-8.5 EEE

By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs because the circuits EEE turnd off to save power and needs time to boot up before sending traffic over the link. This time is called "Wakeup Time". To achieve minimal latency, devices can use LLDP to exchange information about their respective Tx and Rx "Wakeup Time", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To show LLDP EEE neighbors:

- 1. Click LLDP, then click EEE to show discover EEE devices.
- 2. Click "Refresh" for manual update web screen.
- 3. Click "Auto-refresh" for auto-update web screen.

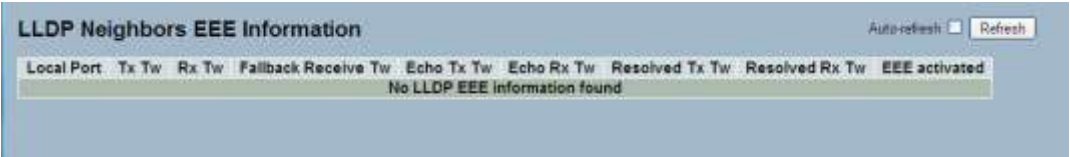


Figure 3-8.5: The LLDP Neighbors EEE information



NOTE: If your network without any devices which enables EEE function then the table will show "No LLDP EEE Information Found".

Parameter Description

Local Port: The port on which LLDP frames are received or transmitted.

Tx Tw: The link partner’s maximum time that transmit path can hold off sending data after reassertion of LPI.

Rx Tw: The link partner’s time that receiver would like the transmitter to hold off allowing time for the receiver to wake from sleep.

Fallback Receive Tw: The link partner’s fallback received Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw: The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partner’s reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw: The link partner's Echo Rx Tw value.

Resolved Tx Tw: The resolved Tx Tw for this link. Note: NOT the link partner.

The resolved value that is the actual "Tx Wakeup Time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw: The resolved Rx Tw for this link. Note: NOT the link partner.

The resolved value that is the actual "Tx Wakeup Time" used for this link (based on EEE information exchanged via LLDP).

EEE activated: Shows if the switch and the link partner have agreed upon which wakeup times to use.

- **Red** - Switch and link partner have not agreed upon wakeup time.
- **Green** - Switch and link partner have agreed upon wakeup time.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the LLDP Neighbors information manually.

3-8.6 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:

1. Click LLDP, and then click Port Statistics to show LLDP counters.
2. Click “Refresh” to manually update the web screen.
3. Click “Auto-refresh” to auto update the web screen.
4. Click “Clear” to clear all counters.

Global Counters

Neighbour entries were last changed at: 2011-01-01 00:00:00 (20488 sec. ago)

Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

Auto-refresh

Refresh

Clear

LLDP Statistics

Local Port	Tx Frames	Rx Frames	Rx Errors	Local Counters				
				Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0

Figure 3-8.6: The LLDP Port Statistics information

Parameter Description

Global Counters

Neighbour Entries Were Last Changed At: It shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbours Entries Added: Shows the number of new entries added since switch reboot.

Total Neighbours Entries Deleted: Shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out: Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port: The port on which LLDP frames are received or transmitted.

Tx Frames: The number of LLDP frames transmitted on the port.

Rx Frames: The number of LLDP frames received on the port.

Rx Errors: The number of received LLDP frames containing some kind of error.

Frames Discarded: If an LLDP frame is received on a port and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the chassis ID or remote port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, a LLDP shutdown frame is received or when the entry ages out.

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs ("Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: The number of well-formed TLVs with an unknown type value.

Org. Discarded: The number of organizationally received TLVs.

Age-Outs: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed and the Age-Out counter is incremented.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear): You can click them to refresh the LLDP Port Statistics information manually. Or press clear to clean up the entries.

3-9 PoE

PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. For example, it could be used for powering IP telephones, wireless LAN access points, and other equipment where it would be difficult or expensive to connect the equipment to main power supply.

3-9.1 Configuration

This page allows the user to inspect and configure the current PoE port settings and show all PoE Supply Watts.

Web Interface

To configure Power over Ethernet in the web interface:

1. Click configuration.
2. Specify the Reserved Power determined and Power Management ode. Specify the PoE or PoE++ and Priority.
3. Click “Apply”.

Power Over Ethernet Configuration

Primary Power Supply [W]	525
PoE Power [W]	180
Power Allocated for PoE	369.6
Power Available for PoE	180
PD Power consumption	0
Retry Time	60 sec(s)

Port	PoE Mode	Priority	Maximum Power [W]	Detection	Reset
*	<>	<>		<>	<input type="checkbox"/>
1	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
2	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
3	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
4	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
5	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
6	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
7	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
8	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
9	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
10	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
11	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
12	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
13	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
14	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
15	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
16	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
17	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
18	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
19	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
20	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
21	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
22	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
23	Enabled	Low	15.4	4-Point	<input type="checkbox"/>
24	Enabled	Low	15.4	4-Point	<input type="checkbox"/>

Apply Reset

Figure 3-9.1: The PoE Configuration

Parameter Description

Power Supply Configuration

Primary Power Supply [W]: The switch can have PoE power supplies. It is used as power source. To determine the amount of power the PD may use, it must define the amount of power the power sources can deliver.

PoE Power: The PoE power supply settings will be shown.

Power Allocated for PoE: The total of maximum power.

Power Available for PoE: Power available for PoE.

PD Power consumption: Show total value of PD power consumption.

Retry Rime: The period (in seconds) for trying to turn on an overloaded PoE port.

Ethernet Port Configuration

Port: This is the logical port number for this row.

PoE Mode: The PoE mode represents the PoE operating mode for the port.

- **Disabled:** PoE disabled for the port.
- **Enabled:** Enables PoE IEEE 802.3af/at.

Priority: The priority represents the ports priority. There are three levels of power priority named low, high, and critical.

The priority is used in case the remote devices require more power than the power supply can deliver. When this happens, the port with the lowest priority will be turned off starting from the port with the highest port number.

Maximum Power: The maximum power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.



NOTE: If you want to set the port support IEEE802.3at, then you can set the maximum allowed value to 30W.

Detection: The detection represents the PoE capacitor detection for the port.

- **Legacy:** Legacy capacitive detection only.
- **4-point:** IEEE 802.3af 4-point detection only.
- **Both:** IEEE 802.3af 4-point detection followed by legacy detection.

Reset: Reset the specific PoE port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-9.2 Status

This page allows the user to inspect the current status for all PoE ports.

Web Interface

To display Power over Ethernet Status in the web interface:

1. Click “Status”.
2. Display Power over Ethernet Status Information.
3. Click “Refresh”.



Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
10	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
11	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
12	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
13	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
14	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
15	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
16	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
17	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
18	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
19	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
20	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
21	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
22	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
23	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
24	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Figure 3-9.2: Power over Ethernet Status

Parameter Description

Local Port: This is the logical port number for this row.

PD Class: The recognition of PD class generates from the current that PD transmits back to the PSE during the detection between PSE and PD. The current is classified by 802.3 at/af protocol. The PD class here is a reference. It is not related to the actual PD power requested.

The PD class that switch read from PD might be inconsistent with the PD specification. There are two reasons for this inconsistency.

1. If the PD supports PoE function, its voltage and current of PD design should follow 802.3 af or 802.3 at protocol. When PD design did not fully follow the protocol, the current PD transmitted back to the switch can't be defined in the classification range that regulated in protocol (in the following table). The switch will define the PD class itself, so it might result in inconsistency.

Classification Category	Classification Current
0 (Type 1)	2.5mA (± 2.5 mA)
1 (Type 1)	10.5mA (± 2.5 mA)
2 (Type 1)	18.5mA (± 2.5 mA)
3 (Type 1)	28mA (± 3 mA)
4 (Type 2)	40mA (± 5 mA)

2. When the current is still unstable while PD connect to PSE but the PD class already has been defined, it might be inconsistent because the PD class is not able to actively adjust. The PD class will adjust after PD is unplugged and then plugged in.
3. The PD class is read at start-up to compensate for the startup power surges and the amount of power allocated to the port during setup.

Power Requested: The power requested shows the requested amount of power the PD wants to be reserved.

Power Allocated: The power allocated shows the amount of power the switch has allocated for the PD.

Power Used: The power used shows how much power the PD currently is using.

Current Used: The power used shows how much current the PD currently is using.

Priority: The priority shows the port's priority configured by the user.

Port Status: The port status shows the port's status.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the PoE port information manually.

3-9.3 Power Delay

This page allows the user to set the delay time of the provided power after the device reboot.

Web Interface

To display Power over Ethernet Status in the web interface:

1. Click Configuration, PoE, and Power delay.
2. Enable the port to the power device.
3. Specify the power providing delay time when reboot.
4. Click "Apply" to apply the change.



NOTE: The delay time and actual time might have about 15 sec gap. The 15 sec gap is for the switch to implement the action of PD detection by PoE, and configuration loading. At the same time, PD process boot up procedure. So, different PDs may result in different gaps on delay time.

POE Power Delay

Port	Delay Mode	Delay Time(0~300 sec)
*	<> ▼	
1	Disable ▼	0
2	Disable ▼	0
3	Disable ▼	0
4	Disable ▼	0
5	Disable ▼	0
6	Disable ▼	0
7	Disable ▼	0
8	Disable ▼	0
9	Disable ▼	0
10	Disable ▼	0
11	Disable ▼	0
12	Disable ▼	0
13	Disable ▼	0
14	Disable ▼	0
15	Disable ▼	0
16	Disable ▼	0
17	Disable ▼	0
18	Disable ▼	0
19	Disable ▼	0
20	Disable ▼	0
21	Disable ▼	0
22	Disable ▼	0
23	Disable ▼	0
24	Disable ▼	0

Apply

Figure 3-9.3: The POE Power Delay

**Parameter
Description**

Port: This is the logical port number for this row.

Delay Mode: Turns on/off the power delay function.

Delay Time (0~300sec): When rebooting, the PoE port will start to provide power to the PD after the delay time.

Button:

- **Apply-** Click “Apply” to apply the change.

3-9.4 Auto Checking

This page allows the user to specify the auto detection parameters to check the linking status between PoE ports and PDs. When it detects the fail connection, it will reboot the remote PD automatically.

Web Interface

To display Power over Ethernet Auto Checking in the web interface:

1. Click Configuration, PoE, and Auto checking.
2. Enable the "Ping Check" function.
3. Specify the PD's IP address, checking interval, retry time, failure action, and reboot time.
4. Click "Apply" to apply the change.

Port	Ping IP Address	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)	Total Reset
1	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
2	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
3	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
4	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
5	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
6	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
7	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
8	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
9	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
10	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
11	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
12	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
13	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
14	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
15	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
16	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
17	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
18	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
19	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
20	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
21	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
22	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
23	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>
24	0.0.0.0	30	3	error=0 ,total=0	Nothing	15	<input type="checkbox"/>

Figure 3-9.4: The POE Auto Checking



CAUTION: When using PoE to power an IP camera or similar device that goes through an initialization period, do not set the "Interval Time" below 20 seconds if the "Failure Action" is set to "Reboot Remote PD". Doing so may prevent the switch from successfully pinging the device and result in a continuous ON-Off-ON-OFF cycle of the PoE power.

Parameter Description

Ping Check: Enables the “Ping Check” function to detect the connection between PoE port and power device. “Disable” will turn off the detection.

Port: This is the logical port number for this row.

Ping IP Address: The PD’s IP address the system should ping.

Interval Time (sec): The device will send checking message to PD each interval time.

Retry Time: When PoE port can’t ping the PD, it will retry to send detection again. When the third time, it will trigger failure action.

Failure Log: Failure loggings counter.

Failure Action: The action when the third fail detection.

- **Nothing-** Keeps pinging the remote PD, but does nothing further.
- **Reboot Remote PD-** Cuts off the power of the PoE port to make PD rebooted.

Reboot time: When PD has been rebooted, the PoE port restored power after the specified time.

Total Reset: Reset total value of the “Failure Log”.

Button:

- **Apply-** Click “Apply” to apply the change.

3-9.5 Scheduling

This page allows the user to make a perfect schedule of PoE power supply. PoE scheduling makes PoE management easier and saves more energy.

Web Interface

To display Power over Ethernet Scheduling in the web interface:

- 1. Click Configuration, PoE, and Scheduling.
- 2. Select the local port and enable.
- 3. Select time and day to supply power.
- 4. Click “Apply” to apply the change.

POE Scheduling

Port	1	2	3	4	5	6	7	8
Status	✖	✖	✖	✖	✖	✖	✖	✖

Port

1

Status

Disable



Select All☐

Hour	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Figure 3-9.5: The POE Scheduling

Parameter Description

Port / Status : This is the logical port number and it’s PoE Scheduling mode.  is “Enable”.  is “Disable”.

Week Day (Sun., Mon.,...): The days of PoE port provide power of a week.

Hour: The time of PoE port provide power of a day.

Button:

- **Apply-** Click “Apply” to apply the change.

3-10 Filtering Data Base

Filtering Data Base Configuration gathers many functions, including MAC Table Information, Static MAC Learning, which cannot be categorized to some function type.

MAC table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time

3-10.1 Configuration

The MAC address table is configured on this page. Set timeouts for entries in the dynamic MAC table and configure the static MAC table here.

Web Interface

To configure MAC address table in the web interface:

Aging Configuration

1. Click "Configuration".
2. Specify the "Disable Automatic Aging and Aging Time".
3. Click "Apply".

MAC Table Learning

1. Click "Configuration".
2. Specify the "Port Members" (Auto, Disable, Secure).
3. Click "Apply".

Static MAC Table Configuration

1. Click "Configuration" and add new static entry.
2. Specify the VLAN IP, Mac address, and Port Members.
3. Click "Apply".

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging ☐

Aging Time seconds

MAC Table Learning

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="button" value="Delete"/>	1	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3- 10.1: The MAC Address Table Configuration

Parameter Description

Aging Configuration: By default, the dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds (e.g. age time). The allowed range is 10 to 1000000 seconds.

Disables the automatic aging of dynamic entries by checking “Disable Automatic Aging”.

Mac Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode so that it cannot be changed by the user. An example of such a module is the MAC-Based authentication under 802.1X. Each port can do learning based upon the following settings:

Auto: Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable: No learning is done.

Secure: Only static MAC entries are learned, all other frames are dropped.



NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode. Otherwise, the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete: Check to delete the entry. It will be deleted during the next save.

VLAN ID: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-10.2 Dynamic MAC Table

Entries in the MAC table are shown on this page. The MAC table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

To display MAC Address Table in the web interface:

1. Click “Dynamic MAC Table”.
2. Specify the VLAN and MAC address.
3. Display MAC address table.

Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static	1	00-40-D8-55-1AF0-00																											
Static	1	33-33-00-00-00-01																											
Static	1	33-33-00-00-00-02																											
Static	1	33-33-FF-12-34-56																											
Static	1	33-33-FF-A8-01-01																											
Dynamic	1	3C-97-0E-16-EB-7E																											

Figure 3- 10.2: The Dynamic MAC Address Table information

Parameter Description

MAC Table Columns

Type: Indicates whether the entry is a static or a dynamic entry.

VLAN: The VLAN ID of the entry.

MAC address: The MAC address of the entry.

Port Members: The ports that are members of the entry.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear, <<, >>): You can click them to refresh or clean up the MAC address entries manually. Press “<< or >>” to go to the next or previous page of the table.



NOTE:

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)
FF-FF-FF-FF-FF-FF : for Broadcast .

3-11 VLAN

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

3-11.1 VLAN Membership

The VLAN membership configuration for the selected switch unit switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs and port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

- 1. Click “VLAN membership Configuration”.
- 2. Specify management VLAN ID from 0-4094.
- 3. Click “Apply”.

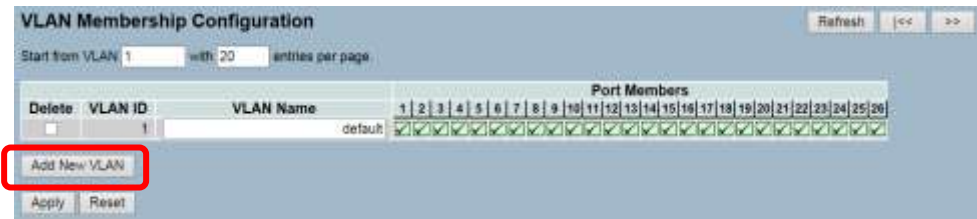


Figure 3-11.1: The VLAN Membership Configuration



**Parameter
Description**

Delete: To delete a VLAN entry, check this box. The entry will be deleted on the selected switch. If none of the ports of this switch are members of a VLAN, then the delete checkbox will be greyed out (you cannot delete that entry during the next save).

VLAN ID: Indicates the ID of this particular VLAN.

VLAN Name: Indicates the name of VLAN. The VLAN name can only contain alphabets or numbers. VLAN name should contain at least one alphabetical letter. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members: A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New VLAN: Click to add a new VLAN ID. An empty row is added to the table and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled on the selected switch unit when you click on "Save". The VLAN is thereafter present on the other switch units, but with no port members. The check box is greyed out when VLAN is displayed on other switches, but the user can add member ports to it.

A VLAN without any port members on any unit will be deleted when you click "Save".

The button can be used to undo the addition of new VLANs.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh, |<<, >>): You can click them to refresh the VLAN entries manually. Or press clear to clean up the VLAN table. Press "|<< or >>" to go to the next or previous page of the table.

3-11.2 Ports

The user can input VID number to each port by using the function in VLAN tag rule setting. The range of VID number is from 1 to 4094. The user also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The ingress filtering rule 1 is “forward only packets with VID matching this port’s configured VID”. The ingress filtering rule 2 is “drop untagged frame”. You can also select the role of each port as access, trunk, or hybrid.

Web Interface

To configure VLAN Port configuration in the web interface:

1. Click “VLAN Port Configuration”.
2. Specify the VLAN port configuration parameters.
3. Click “Apply”.

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	<input type="checkbox"/>	<>	<>	
1	Unaware	<input type="checkbox"/>	All	Hybrid	1
2	Unaware	<input type="checkbox"/>	All	Hybrid	1
3	Unaware	<input type="checkbox"/>	All	Hybrid	1
4	Unaware	<input type="checkbox"/>	All	Hybrid	1
5	Unaware	<input type="checkbox"/>	All	Hybrid	1
6	Unaware	<input type="checkbox"/>	All	Hybrid	1
7	Unaware	<input type="checkbox"/>	All	Hybrid	1
8	Unaware	<input type="checkbox"/>	All	Hybrid	1
9	Unaware	<input type="checkbox"/>	All	Hybrid	1
10	Unaware	<input type="checkbox"/>	All	Hybrid	1
11	Unaware	<input type="checkbox"/>	All	Hybrid	1
12	Unaware	<input type="checkbox"/>	All	Hybrid	1
13	Unaware	<input type="checkbox"/>	All	Hybrid	1
14	Unaware	<input type="checkbox"/>	All	Hybrid	1
15	Unaware	<input type="checkbox"/>	All	Hybrid	1
16	Unaware	<input type="checkbox"/>	All	Hybrid	1
17	Unaware	<input type="checkbox"/>	All	Hybrid	1
18	Unaware	<input type="checkbox"/>	All	Hybrid	1
19	Unaware	<input type="checkbox"/>	All	Hybrid	1
20	Unaware	<input type="checkbox"/>	All	Hybrid	1
21	Unaware	<input type="checkbox"/>	All	Hybrid	1
22	Unaware	<input type="checkbox"/>	All	Hybrid	1
23	Unaware	<input type="checkbox"/>	All	Hybrid	1
24	Unaware	<input type="checkbox"/>	All	Hybrid	1
25	Unaware	<input type="checkbox"/>	All	Hybrid	1
26	Unaware	<input type="checkbox"/>	All	Hybrid	1

ApplyReset

Figure 3-11.2: The VLAN Port Configuration

Parameter Description

Ethertype for Custom S-ports: This field specifies the Ethertype used for custom S-ports. This is a global setting for all the custom S-ports. The custom Ethertype enables the user to change the Ethertype value on a port in order to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

Port: This is the logical port number of this row.

Port Type: The follow are different port types: Unaware, Customer port (C-port), Service port (S-port), Custom Service port (S-custom-port). If the port type is “Unaware”, all of the frames are classified to the port VLAN ID and the tags are not removed.

Ingress Filtering: Evoke t o enable ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, the ingress filtering is disabled (no checkmark).

Frame Type: Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to “All”.

Egress Rule: Determines what device the port connects to. If the port connects to VLAN-unaware devices (e.g. terminal/work station), the access link should be used. If the port connect to VLAN-aware devices (e.g. switch connect to switch), the trunk link should be used. Hybrid link is used for more flexible application.

- **Hybrid:** If the tag of tagged frame is as the same as PVID, the tag of the frame will be removed. The frame become an untagged frame and transmitted. Any other tagged frame whose tag value is different from PVID are transmitted directly.
- **Trunk:** All tagged frames with any tag value are transmitted.
- **Access:** The tag of any tagged frame will be removed to become an untagged frame. These untagged frames will be transmitted.

Port VLAN Mode: Configures the port VLAN mode. The allowed values are “None” or “Specific”. This parameter affects VLAN ingress and egress processing. If “None” is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. If “Specific” (the default value) is selected, a port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the port VLAN ID. If “VLAN Awareness” is disabled, all frames received on the port are classified to the port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID: Configures the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1.



NOTE: The port must be a member of the same VLAN as the port VLAN ID.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-11.3 Switch
Status

The function switch status gathers the information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN membership status in the web interface:

- 1. Click “VLAN Membership”.
- 2. Specify the Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.
- 3. Display membership information.



Figure 3-11.3: The VLAN Membership Status for Combined users




Parameter
Description

VLAN USER (You can scroll to select one kind VLAN user as below): “VLAN User” module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently, we support the following VLAN user types:

- **Web/SNMP:** These are referred to as static.
- **NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
- **MVRP:** Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.
- **GVRP:** GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.
- **Voice VLAN:** Voice VLAN is a VLAN configured especially for voice traffic typically originating from IP phones.
- **MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- **MSTP:** The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

VLAN ID: Indicates the ID of this particular VLAN.

Port Members: A row of check boxes for each port is displayed for each VLAN ID.

- If a port is included in a VLAN, an image  will be displayed.
- If a port is included in a forbidden port list, an image  will be displayed.
- If a port is included in a forbidden port list and dynamic VLAN user register VLAN on the same forbidden port, then conflict port will be displayed as .

VLAN Membership: The VLAN membership status page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a combo box). When “All VLAN Users” are selected, by default, it shall show this information for all the VLAN users. The VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the VLAN entries manually.

3-11.4 Port Status

The function Port Status gathers the information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN Port Status in the web interface:

1. Click “VLAN Port Status”.
2. Specify the Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.
3. Display port status information.



Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No

Figure 3-11.4: The VLAN Port Status for Static user

Parameter Description

Port: The logical port for the settings contained in the same row.

PVID: Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

Port Type: Shows the port type. Port type can be any of Unaware, C-port, S-port, or Custom S-port.

If port type is “Unaware”, all frames are classified to the port VLAN ID and tags are not removed. C-port is “Customer Port”. S-port is “Service Port”. Custom S-port is “S-port with Custom TPID”.

Ingress Filtering: Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type: Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, the untagged frames received on that port are discarded.

Tx Tag: Shows egress filtering frame status whether tagged or untagged.

UVID: Shows UVID (untagged VLAN ID). The port's UVID determines the packet's behavior at the egress side.

Conflicts: Shows status of conflicts whether they exists or not. When a volatile VLAN sser requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the VLAN Port Status information manually.

3-11.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

3-11.5.1 Private VLANs Membership

The private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each private VLAN can be added or removed here. Private VLANs are based on the source port mask and there are no connections to VLANs. This means that the VLAN IDs and the private VLAN IDs can be identical. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.

Web Interface

To configure Private VLAN configuration in the web interface:

- 1. Click “Add New Private VLAN Configuration”.
- 2. Specify the private VLAN ID and port members.
- 3. Click “Apply”.

Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members																									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<div>Add New Private VLAN</div>																											
<div>ApplyReset</div>																											

Figure 3-11.5.1: The Private VLAN Membership Configuration

Parameter Description

Delete: Check this box to delete a private VLAN entry. The entry will be deleted during the next save.

PVLAN ID: Indicates the ID of this particular private VLAN.

Port Members: A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a private VLAN, check the box. To remove or exclude the port from the private VLAN, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New Private VLAN: Click to add a new private VLAN ID. An empty row is added to the table and the private VLAN can be configured as needed.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-11.5.2 Port Isolation

Port isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and private VLAN.

Web Interface

- To configure Port Isolation configuration in the web interface:
- 1. Click “VLAN”, then “Port Isolation”.
 - 2. Evoke which port want to enable port isolation.
 - 3. Click “Apply”.

Port Isolation Configuration

Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Reset

Figure 3-11.5.2: The Port Isolation Configuration

Parameter Description

Port Numbers: A check box is provided for each port of a private VLAN. When checked, the port isolation is enabled on that port. When unchecked, the port isolation is disabled on that port. By default, the port isolation is disabled on all ports.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-11.6 MAC-Based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A most common way of grouping VLAN members is by port, hence the name “Port-based VLAN”. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do. This causes security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure and flexible network access for terminal devices.

3-11.6.1 Configuration

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries, and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click “MAC address-based VLAN Configuration” and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click “Apply”.

MAC-based VLAN Membership Configuration Refresh |<< >>

Delete	MAC Address	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Currently no entries present																												

Add new entry

Apply Reset

MAC-based VLAN Membership Configuration Refresh |<< >>

Delete	MAC Address	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	00-00-00-00-00-00	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new entry

Apply Reset

Figure 3-11.6.1: The MAC-Based VLAN Membership Configuration

Parameter Description

Delete: To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch.

MAC Address: Indicates the MAC address.

VLAN ID: Indicates the VLAN ID.

Port Members: A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New MAC-based VLAN: Click to add a new MAC-based VLAN entry. An empty row is added to the table and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. The legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled on the selected switch unit when you click on "Save". A MAC-based VLAN without any port members on any unit will be deleted when you click "Save".

The button can be used to undo the addition of new MAC-based VLANs.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset** – Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-11.6.2 Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently, we support following VLAN User types:

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To display MAC-based VLAN configured in the web interface:

- 1. Click “MAC-based VLAN Status”.
- 2. Specify the “Static NAS Combined”.
- 3. Display MAC-based information.



Figure 3-11.6.2: The MAC-based VLAN Membership Status for User Static

Parameter
Description

- MAC Address:** Indicates the MAC address.
- VLAN ID:** Indicates the VLAN ID.
- Port Members:** Port members of the MAC-based VLAN entry.
- Auto-refresh:** Evoke the auto-refresh icon to refresh the information automatically.
- Upper right icon (Refresh):** You can click them to refresh the MAC-based VLAN Membership information manually.

3-11.7 Protocol-
Based VLAN

This section describes protocol-based VLAN. The switch support protocol include Ethernet LLC SNAP Protocol.

LLC: The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the “Data Link Layer” (which is layer 2 itself, just above the physical layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that makes it possible for several network protocols (IP, IPX, Decnet, and Appletalk) to coexist within a multipoint network and to be transported over the same network media. It also provides flow control and automatic repeat request ARQ error management mechanisms.

SNAP: The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11, and other IEEE 802 physical network layers, as well as, with non-IEEE 802 physical network layers such as FDDI that uses 802.2 LLC.

3-11.7.1 Protocol
to Group

This page allows you to add new protocols to group name (unique for each group) mapping entries. It also allows you to view or delete already mapped entries for the selected switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

- 1. Click “Protocol -based VLAN Configuration” and add a new entry.
- 2. Specify the Ethernet LLC SNAP protocol and group name.
- 3. Click “Apply”.



Figure 3-11.7.1: The Protocol to Group Mapping Table

Parameter Description

Delete: To delete a protocol to group name map entry, check this box. The entry will be deleted on the switch during the next save.

Frame Type: Frame type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP



NOTE: On changing the frame type field - The valid value of the following text field will vary depending on the new frame type you selected.

Value: The valid value that can be entered in this text field depends on the option selected from the preceding frame type selection menu. Below are the criteria for three different frame types.

1. **For Ethernet:** Values in the text field when Ethernet is selected as a frame type is called etype. Valid values for etype ranges from 0x0600-0xffff.
2. **For LLC:** Valid value in this case is comprised of two different sub-values.
 - a. DSAP: 1-byte long string (0x00-0xff)
 - b. SSAP: 1-byte long string (0x00-0xff)
3. **For SNAP:** Valid value in this case also is comprised of two different sub-values.
 - a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
 - b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet Type (EtherType) field value for the protocol running on top of SNAP. If the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if the value of OUI field is 00-00-00, then value of PID will be etype (0x0600-0xffff) . If the value of OUI is other than 00-00-00, then the valid value of PID will be any value from 0x0000 to 0xffff.

Group Name: A valid group name is a unique 16-character long string for every entry. It consists of a combination of alphabets (a-z or A-Z) and integers (0-9).



NOTE: Special character and underscore (_) are not allowed.

Adding a New Group to VLAN Mapping Entry: Click this to add a new entry in mapping table. An empty row is added to the table. Frame Type, Value, and the Group Name can be configured as needed. The button can be used to undo the addition of new entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh): You can click them to refresh the protocol group mapping information manually.

3-11.7.2 Group to VLAN

This section allows you to map an already configured group name to a VLAN for the selected switch.

Web Interface

To display Group Name to VLAN mapping table configured in the web interface:

1. Click “Group Name VLAN Configuration” and add new entry.
2. Specify the “Group Name” and “VLAN ID”.
3. Click “Apply”.

The figure consists of two screenshots of a web interface titled "Group Name to VLAN mapping Table".

The top screenshot shows the interface with the "Add new entry" button highlighted by a red box. Below the button are "Apply" and "Reset" buttons. The table below has columns for "Delete", "Group Name", "VLAN ID", and "Port Members" (ports 1 through 26). The text "No Group entries" is displayed in the table area.

The bottom screenshot shows the same interface after clicking "Add new entry". The "Group Name" and "VLAN ID" fields are now empty input boxes. The "Port Members" section shows a grid of checkboxes for each port from 1 to 26.

Figure 3-11.7.2: The Group Name of VLAN Mapping Table

Parameter Description

Delete: To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name: A valid Group Name is a string of at most 16 characters, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be perused by any other existing mapping entry on this page.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members: A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New Group to VLAN mapping entry: Click this option to add a new entry in mapping table. An empty row is added to the table. The Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the Protocol Group Mapping information manually.

3-12 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data to ensure the transmission priority of voice traffic and voice quality.

3-12.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice and one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

- 1. Select “Enabled” in the Voice VLAN Configuration.
- 2. Specify VLAN ID Aging Time Traffic Class.
- 3. Specify (Port Mode, Security, Discovery Protocol) in the Port Configuration.
- 4. Click “Apply”.

Voice VLAN Configuration

Mode

Disabled

VLAN ID

1000

Aging Time

86400

seconds

Traffic Class

7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI
19	Disabled	Disabled	OUI
20	Disabled	Disabled	OUI
21	Disabled	Disabled	OUI
22	Disabled	Disabled	OUI
23	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI
25	Disabled	Disabled	OUI
26	Disabled	Disabled	OUI

Apply

Reset

Figure 3-12.1: The Voice VLAN Configuration

Parameter Description

Mode: Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

- **Enabled:** Enable Voice VLAN mode operation.
- **Disabled:** Disable Voice VLAN mode operation.

VLAN ID: Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time: Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode: Indicates the Voice VLAN port mode.

When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.

Possible port modes are:

- **Disabled:** Disjoin from Voice VLAN.
- **Auto:** Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- **Forced:** Force join to Voice VLAN.

Port Security: Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

- **Enabled:** Enable Voice VLAN security mode operation.
- **Disabled:** Disable Voice VLAN security mode operation.

Port Discovery Protocol: Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the auto detect process. Possible discovery protocols are:

- **OUI:** Detect telephony device by OUI address.
- **LLDP:** Detect telephony device by LLDP.
- **Both:** Both OUI and LLDP.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

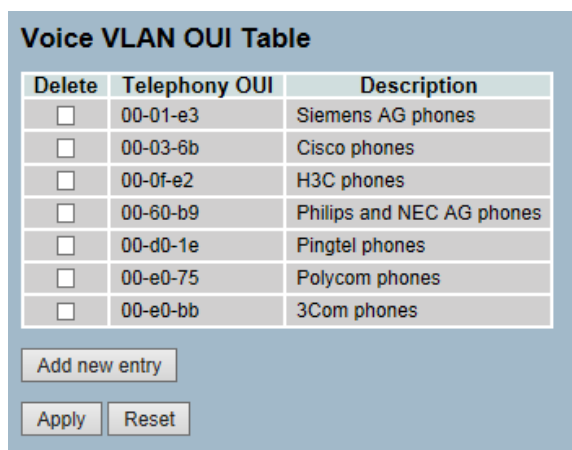
3-12.2 OUI

The section describes how to Configure VOICE VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Select "Add new entry", "Delete" in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click "Apply".



Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Add new entry

Apply Reset

Figure 3-12.2: The Voice VLAN OUI Table

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description: The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Add New Entry: Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, Description.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**– Click "Reset" to undo any changes made locally and revert back to previously saved values.



NOTE: All non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.
For example: When Pkts keep entering the port, add a new OUI entry. It can help this OUI match current Pkts, then it must be found the packet will be forward.

3-13 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN (e.g. end stations and switches can register and de-register attribute values, such as VLAN Identifiers, with each other). In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

3-13.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure GARP Port Configuration in the web interface:

1. Click GARP configures.
2. Specify GARP Configuration Parameters.
3. Click “Apply”.

Port	Join Timer	Leave Timer	Leave All Timer	Application	Attribute Type	GARP Applicant
1	200	600	10000	GVRP	VLAN	normal-participant
2	200	600	10000	GVRP	VLAN	normal-participant
3	200	600	10000	GVRP	VLAN	normal-participant
4	200	600	10000	GVRP	VLAN	normal-participant
5	200	600	10000	GVRP	VLAN	normal-participant
6	200	600	10000	GVRP	VLAN	normal-participant
7	200	600	10000	GVRP	VLAN	normal-participant
8	200	600	10000	GVRP	VLAN	normal-participant
9	200	600	10000	GVRP	VLAN	normal-participant
10	200	600	10000	GVRP	VLAN	normal-participant
11	200	600	10000	GVRP	VLAN	normal-participant
12	200	600	10000	GVRP	VLAN	normal-participant
13	200	600	10000	GVRP	VLAN	normal-participant
14	200	600	10000	GVRP	VLAN	normal-participant
15	200	600	10000	GVRP	VLAN	normal-participant
16	200	600	10000	GVRP	VLAN	normal-participant
17	200	600	10000	GVRP	VLAN	normal-participant
18	200	600	10000	GVRP	VLAN	normal-participant
19	200	600	10000	GVRP	VLAN	normal-participant
20	200	600	10000	GVRP	VLAN	normal-participant
21	200	600	10000	GVRP	VLAN	normal-participant
22	200	600	10000	GVRP	VLAN	normal-participant
23	200	600	10000	GVRP	VLAN	normal-participant
24	200	600	10000	GVRP	VLAN	normal-participant
25	200	600	10000	GVRP	VLAN	normal-participant
26	200	600	10000	GVRP	VLAN	normal-participant

Figure 3-13.1: The GARP Port Configuration

Parameter Description

Port: The Port column shows the list of ports for which you can configure GARP settings. There are 2 types of configuration settings which can be configured on per port bases.

- Timer Values
- Application
- Attribute Type
- GARP Applicant

Timer Values: To set the GARP join timer, leave timer and leave all timers, units are Micro-second. Three different timers can be configured on this page:

- **Join Timer:** The default value for Join timer is 200ms.
- **Leave Timer:** The range of values for Leave Time is 600-1000ms. The default value for Leave Timer is 600ms.
- **Leave All Timer:** The default value for Leave All Timer is 10000ms

Application: Currently only supported application is GVRP.

Attribute Type: Currently only supported Attribute Type is VLAN.

GARP Applicant: This configuration is used to configure the Applicant state machine behavior for GARP on a particular port locally.

- **Normal-participant:** In this mode, the Applicant state machine will operate normally in GARP protocol exchanges.
- **Non-participant:** In this mode, the Applicant state machine will not participate in the protocol operation.

The default configuration is normal participant.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-13.2 Statistics

The section describes how to port statistics of GARP for all switch ports. The port statistics relate to the currently selected unit, as reflected by the page header.

Web Interface

To display GARP Port statistics in the web interface:

- 1. Click GARP statistics.
- 2. Scroll which port you want To display the GARP Counter information.
- 3. Click Refresh to modify the GARP statistics information.

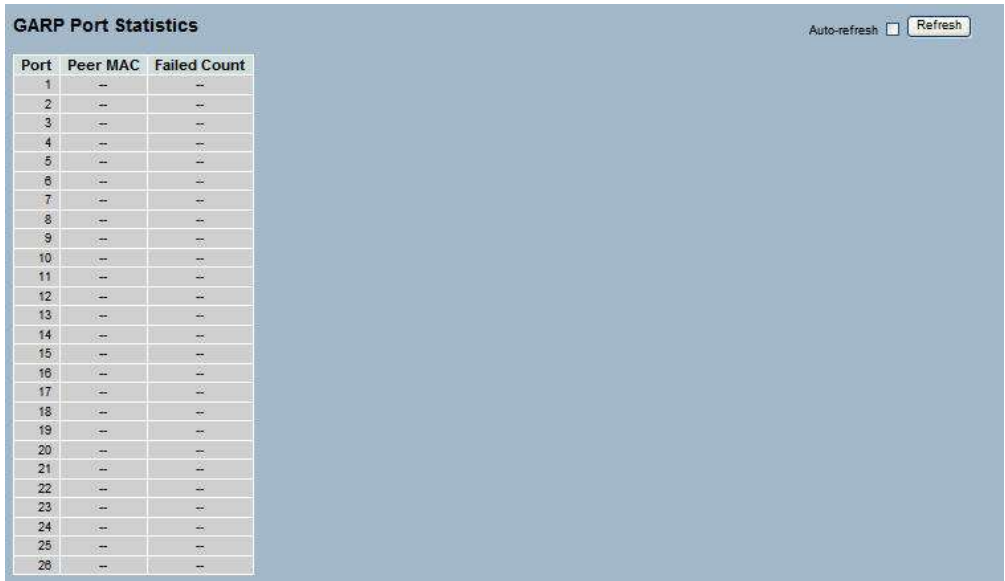


Figure 3-13.2: The GARP Port Statistics

Parameter Description

- Port:** The Port column shows the list of all ports for which per port GARP statistics are shown.
- Peer MAC:** Peer MAC is MAC address of the neighbour Switch from with GARP frame is received.
- Failed Count:** Explains Failed count here.
- Auto-refresh:** Evoke the auto-refresh icon to refresh the information automatically.
- Upper right icon (Refresh):** You can click them to refresh the GARP Port Statistics information manually.

3-14 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP). It is mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function to provide the VLAN registration service through a GARP application. It makes use of the GARP Information Declaration (GID) to maintain the ports associated with their attribute database and the GARP Information Propagation (GIP) to communicate among switches and end stations. With the GID information and GIP, the GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to set up and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

3-14.1 Configuration

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure GVRP Port Configuration in the web interface:

1. Click “GVRP Configure”.
2. Specify the GVRP configuration parameters.
3. Click “Apply”.

Port	GVRP Mode	GVRP rrole
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable
7	Disable	Disable
8	Disable	Disable
9	Disable	Disable
10	Disable	Disable
11	Disable	Disable
12	Disable	Disable
13	Disable	Disable
14	Disable	Disable
15	Disable	Disable
16	Disable	Disable
17	Disable	Disable
18	Disable	Disable
19	Disable	Disable
20	Disable	Disable
21	Disable	Disable
22	Disable	Disable
23	Disable	Disable
24	Disable	Disable
25	Disable	Disable
26	Disable	Disable

Figure 3-14.1: The GVRP Global Configuration

Parameter Description

GVRP Mode: GVRP Mode is a global setting. To enable the GVRP globally, select “Enable” from menu and to disable GVRP globally, select “Disable”.

Port: The port column shows the list of ports that you can configure per port GVRP settings. There are three configuration settings which can be configured on per port bases.

1. **GVRP Mode:** This configuration is to enable/disable GVRP Mode on a particular port locally.
 - a. **Disable:** Select “Disable” to disable GVRP mode on this port.
 - b. **Enable:** Select “Enable” to enable GVRP mode on this port.
 - i. The default value of configuration is “Disable”.
2. **GVRP Rrole:** This configuration is used to configure restricted role on an interface.
 - a. **Disable:** Select “Disable” to disable GVRP rrole on this port.
 - b. **Enable:** Select “Enable” to enable GVRP rrole on this port.
 - i. The default configuration is “Disable”.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the GVRP Global configuration information manually.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-14.2 Statistics

The section describes the basic GVRP port statistics for all switch ports. The statistics relate to the currently selected unit as reflected by the page header.

Web Interface

To display GVRP Port statistics in the web interface:

- 1. Click “GVRP Statistics”.
- 2. Scroll which port you want to display the GVRP counter information.
- 3. Click “Refresh” to modify the GVRP statistics information.

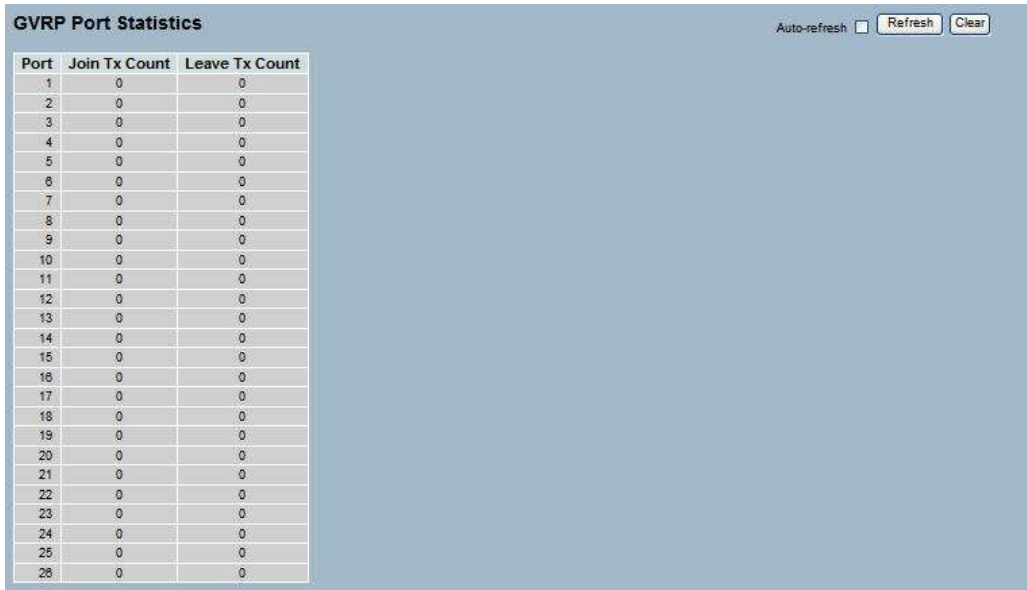


Figure 3-14.2: The GVRP Port Statistics

Parameter Description

Port: The port column shows the list of ports for which you can see port counters and statistics.

Join TX Count: Explains “Join TX Count” here.

Leave TX Count: Explains “Leave TX Count” here.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the GVRP port statistics information manually.

3-15 QoS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device to provide queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority are in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU, even when all the QoS class queues are congested.

3-15.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports. The settings are related to the currently selected unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, and Port Classification.
2. Scroll to select QoS class, DP Level, PCP, and DEI parameters.
3. Click “Apply” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<> ▾	<> ▾	<> ▾	<> ▾		<input type="checkbox"/>
1	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
2	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
3	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
4	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
5	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
6	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
7	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
8	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
9	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
10	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
11	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
12	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
13	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
14	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
15	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
16	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
17	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
18	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
19	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
20	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
21	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
22	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
23	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
24	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
25	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>
26	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>

Apply Reset

Figure 3-15.1: The QoS Configuration

Parameter Description

Port: The port number for which the configuration below applies.

QoS class: Controls the default QoS class (e.g. the QoS class for frames not classified in any other way). There is a one to one mapping between QoS class, queue, and priority. A QoS class of zero (0) has the lowest priority.

DP level: Controls the default DP level (e.g. the DP level for frames not classified in any other way).

PCP: Controls the default PCP for untagged frames.

DEI: Controls the default DEI for untagged frames.

Tag Class: Shows the classification mode for tagged frames on this port.

- **Disabled:** Use the default QoS class and DP level for tagged frames.
- **Enabled:** Use the mapped versions of PCP and DEI for tagged frames.
- Click on the mode in order to configure the mode and/or mapping.

DSCP Based: Click to enable DSCP Based QoS Ingress Port Classification.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset** – Click “Reset” to undo any changes made locally and revert back to previously saved values.



NOTE: DP level: Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device to provide congestion control guarantees to the frame, according to what was configured for that specific DP level.

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

Actual PCP is Pri column in Vlan tag packet. DEI is cfi column PCP value from 0~7. It can be used for priority definition. DEI value is 0 or 1. It is settable and map to the DP value of 0 or 1. When the ingress Qos class value is the same, then through DP level value to define the priority. DP value larger will be dropped first.

Ex: From port 1 input 1G pkts, egress port 7 rate be set with 500M. Port 1 pkts will includes two kinds packet:

- a. PCP & DEI = 0 0, via configured map to Qos class & DP level = 1 , 0
- b. PCP & DEI = 0 1, via configured map to Qos class & DP level = 1 , 1

Result will find (a) Packet all past, and (b) packets all drop.

3-15.2 Port Policing

This section provides an overview of QoS ingress port policers for all switch ports. The port policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

Web Interface

To display the QoS port schedulers in the web interface:

1. Click Configuration, QoS, and Port Policing.
2. Evoke which port need to enable the QoS ingress port policers and type the rate limit condition.
3. Scroll to select the rate limit unit with kbps, mbps, fps, or kfps.
4. Click “Apply” to save the configuration.

Port	Mode	Rate	Unit	Flow Control
*	<input type="checkbox"/>	<input type="text"/>	<input type="text"/> <input type="text"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
25	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>
26	<input type="checkbox"/>	500	kbps <input type="text"/>	<input type="checkbox"/>

Figure 3-15.2: The QoS Ingress Port Policers Configuration

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: To evoke which port you need to enable the QoS ingress port policers function.

Rate: To set the rate limit value for this port. The default is 500.

Unit: Scroll to select the unit of rate - kbps, Mbps, fps, and kfps. The default is kbps.

Flow Control: Evoke to enable or disable flow control on port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.3 Port Scheduler

This section provides an overview of QoS egress port schedulers for all switch ports and the ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Schedulers in the web interface:

- 1. Click Configuration, QoS, then Port Schedulers.
- 2. Display the QoS egress port schedulers.

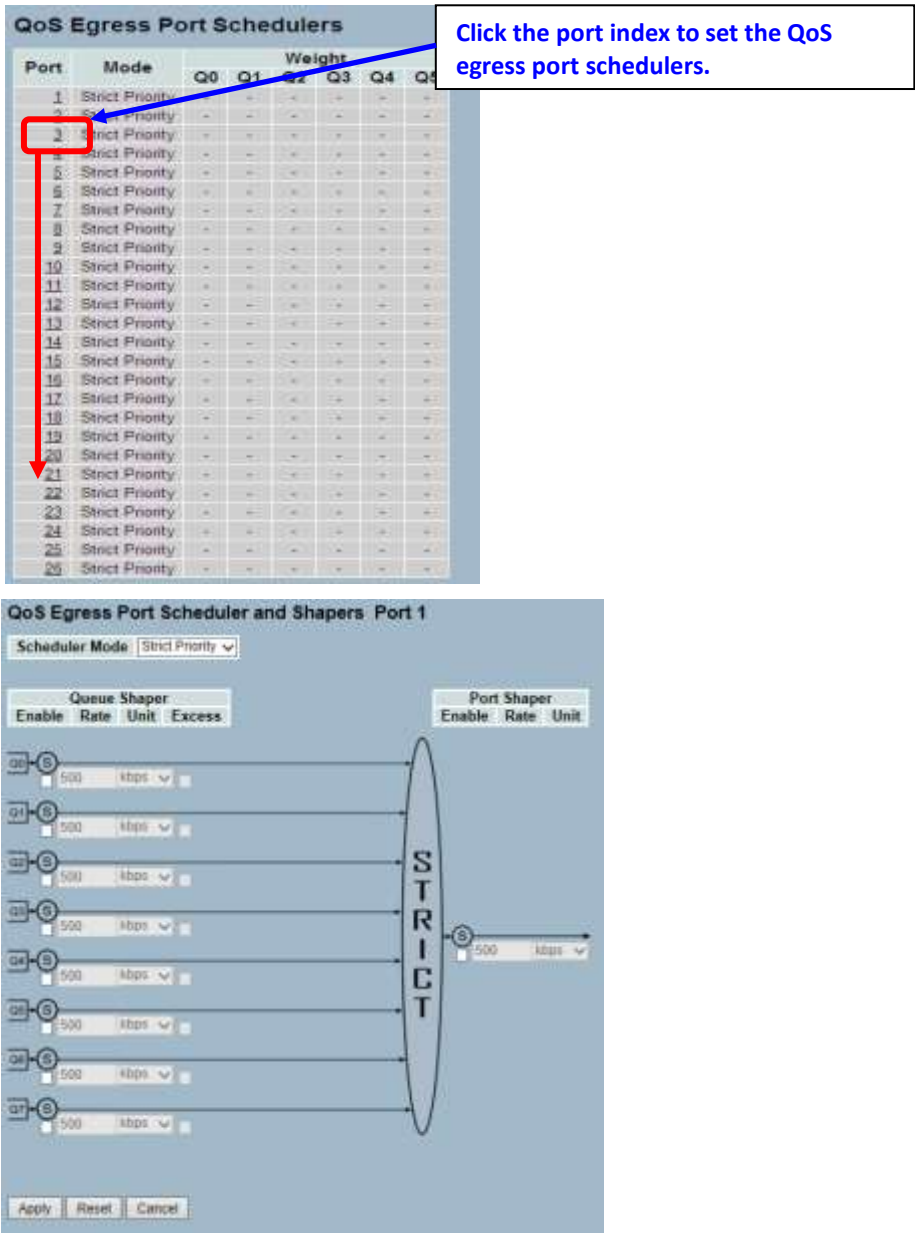


Figure 3-15.3: The QoS Egress Port Schedules

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: **Weighted**

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps

Diagram: A central vertical oval labeled "D W R R I C T" is flanked by two vertical ovals labeled "S T R I C T". Arrows point from the "Queue Scheduler" section to the central oval and from the "Port Shaper" section to the right oval.

Buttons: Apply, Reset, Cancel

If you select the scheduler mode with weighted, then the screen will change as the figure.

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: Shows the scheduling mode for this port.

Weight (Qn): Shows the weight for this queue and port.

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the unit is "Kbps", and it is restricted to 1-1000 when the unit is "Mbps".

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "Kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if scheduler mode is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the unit is "kbps", and it is restricted to 1-1000 when the unit is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.4 Port Shaping

This section provides an overview of QoS egress port shaping for all switch ports. The user could also get all detailed information of the ports to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Shapers in the web interface:

- 1. Click Configuration, QoS, and Port Shapers.
- 2. Display the QoS egress port shapers.

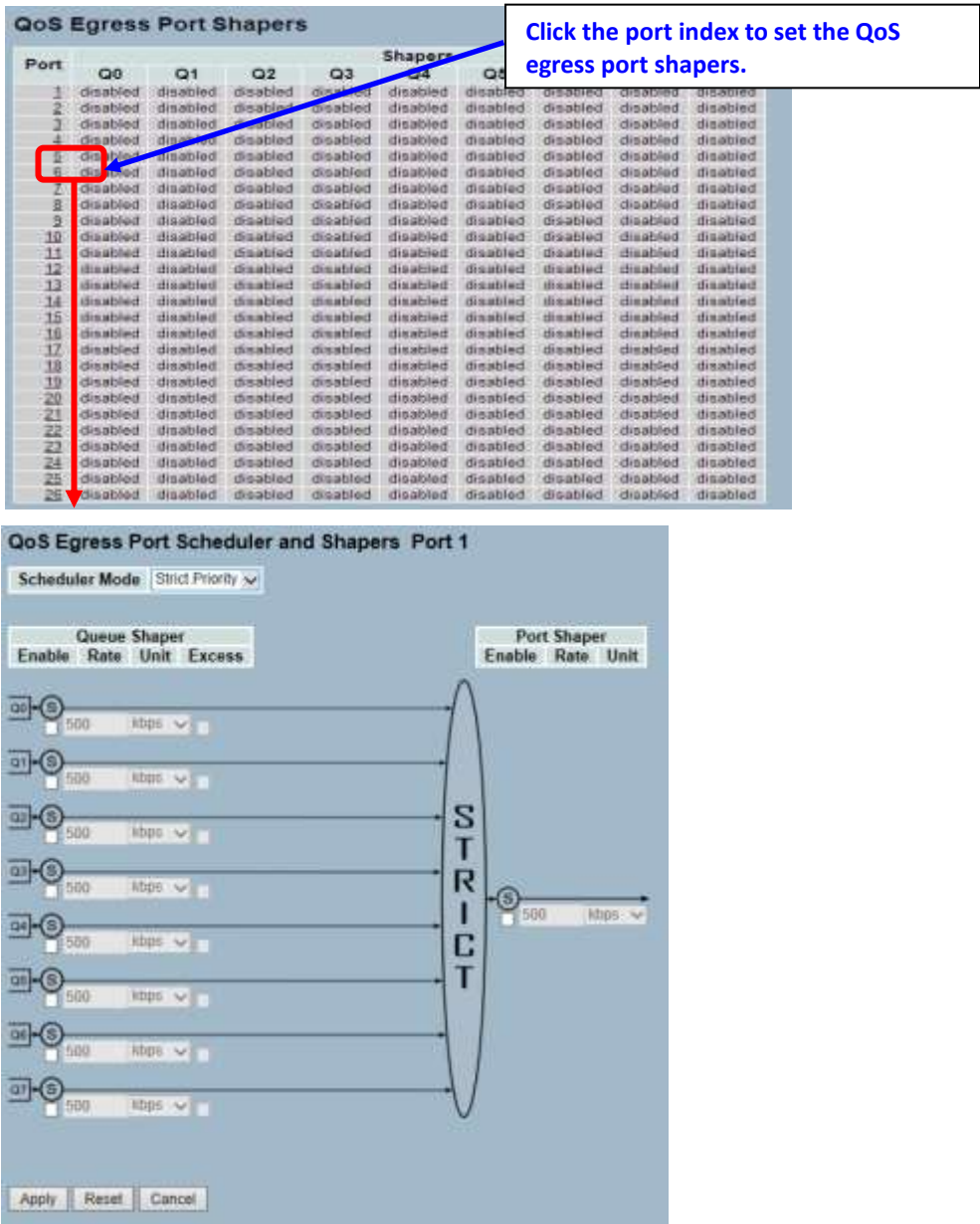


Figure 3-15.4: The QoS Egress Port Shapers

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: **Weighted**

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps

Apply Reset Cancel

Diagram: A diagram showing 8 queues (Q0-Q7) feeding into a central vertical oval labeled "D W R R I C T". To the right of this oval is a vertical oval labeled "S T R I C T". A single line from the "S T R I C T" oval leads to a Port Shaper box with a rate of 500 kbps.

Annotation: A blue arrow points from the "Weighted" dropdown menu to a text box that says: "If you select the scheduler mode with weighted, then the screen will change as the figure."

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Shapers (Qn): Shows "Disabled" or actual queue shaper rate (e.g. "800 Mbps").

Shapers (Port): Shows "Disabled" or actual port shaper rate – (e.g. "800 Mbps").

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the unit is "kbps", and it is restricted to 1-1000 when the unit is "Mbps".

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is 17. This value is restricted to 1-100.

This parameter is only shown if scheduler mode is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if scheduler mode is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the unit is "kbps", and it is restricted to 1-1000 when the unit is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.5 Port Tag Remark

The section provides user to get an overview of QoS egress port tag remarking for all switch ports. The ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, and Port Tag Remarking.

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Classified

Apply Reset Cancel

Figure 3-15.5: The Port Tag Remarking

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

Mode: Shows the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

Tag Remarking Mode: To scroll to select the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.

- **Mapped:** Use mapped versions of QoS class and DP level.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.
- **Cancel** – Click “Cancel” to cancel the changes.

3-15.6 Port DSCP

The section sets the QoS Port DSCP configuration that allowed the user to configure the basic QoS Port DSCP configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS, and Port DSCP.
2. Evoke to enable or disable the ingress translate and scroll the classify parameter configuration.
3. Scroll to select egress rewrite parameters.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input type="checkbox"/>	Disable	Disable
10	<input type="checkbox"/>	Disable	Disable
11	<input type="checkbox"/>	Disable	Disable
12	<input type="checkbox"/>	Disable	Disable
13	<input type="checkbox"/>	Disable	Disable
14	<input type="checkbox"/>	Disable	Disable
15	<input type="checkbox"/>	Disable	Disable
16	<input type="checkbox"/>	Disable	Disable
17	<input type="checkbox"/>	Disable	Disable
18	<input type="checkbox"/>	Disable	Disable
19	<input type="checkbox"/>	Disable	Disable
20	<input type="checkbox"/>	Disable	Disable
21	<input type="checkbox"/>	Disable	Disable
22	<input type="checkbox"/>	Disable	Disable
23	<input type="checkbox"/>	Disable	Disable
24	<input type="checkbox"/>	Disable	Disable
25	<input type="checkbox"/>	Disable	Disable
26	<input type="checkbox"/>	Disable	Disable

Apply Reset

Figure 3-15.6: The QoS Port DSCP Configuration

Parameter Description

Port: The port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress: In ingress settings, you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in ingress:

1. **Translate:** To enable the ingress translation, click the checkbox.
2. **Classify:** Classification for a port has 4 different values.
 - a. **Disable:** No ingress DSCP classification.
 - b. **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0.
 - c. **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP translation window for the specific DSCP.
 - d. **All:** Classify all DSCP.

Egress: Port egress rewriting can be one of below parameters.

- **Disable:** No egress rewrite.
- **Enable:** Rewrite enable without remapped.
- **Remap:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.7 DSCP-Based QoS

The section configures the DSCP-Based QoS mode. The user can configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS, and DSCP-Based QoS.
2. Evoke to enable or disable the DSCP for Trust.
3. Scroll to select QoS class and DPL parameters.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<> ▼	<> ▼
0 (BE)	<input type="checkbox"/>	0 ▼	0 ▼
1	<input type="checkbox"/>	0 ▼	0 ▼
2	<input type="checkbox"/>	0 ▼	0 ▼
3	<input type="checkbox"/>	0 ▼	0 ▼
4	<input type="checkbox"/>	0 ▼	0 ▼
5	<input type="checkbox"/>	0 ▼	0 ▼
6	<input type="checkbox"/>	0 ▼	0 ▼
7	<input type="checkbox"/>	0 ▼	0 ▼
8 (CS1)	<input type="checkbox"/>	0 ▼	0 ▼
9	<input type="checkbox"/>	0 ▼	0 ▼
10 (AF11)	<input type="checkbox"/>	0 ▼	0 ▼
11	<input type="checkbox"/>	0 ▼	0 ▼
12 (AF12)	<input type="checkbox"/>	0 ▼	0 ▼
13	<input type="checkbox"/>	0 ▼	0 ▼
14 (AF13)	<input type="checkbox"/>	0 ▼	0 ▼
15	<input type="checkbox"/>	0 ▼	0 ▼
16 (CS2)	<input type="checkbox"/>	0 ▼	0 ▼
17	<input type="checkbox"/>	0 ▼	0 ▼
18 (AF21)	<input type="checkbox"/>	0 ▼	0 ▼
59	<input type="checkbox"/>	0 ▼	0 ▼
60	<input type="checkbox"/>	0 ▼	0 ▼
61	<input type="checkbox"/>	0 ▼	0 ▼
62	<input type="checkbox"/>	0 ▼	0 ▼
63	<input type="checkbox"/>	0 ▼	0 ▼

Apply Reset

Figure 3-15.7: The DSCP-Based QoS Ingress Classification Configuration

**Parameter
Description**

DSCP: The maximum number of supported DSCP values is 64.

Trust: Click to check if the DSCP value is trusted.

QoS Class: QoS Class value can be any of (0-7).

DPL: Drop Precedence Level (0-3).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.8 DSCP Translation

The section configures the basic QoS DSCP translation settings for all switches. DSCP translation can be done in ingress or egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS, and DSCP Translation.
2. Scroll to set the ingress translate and egress remap DP0 and remap DP1 parameters.
3. Evoke to enable or disable “Classify”.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)
13	13	<input type="checkbox"/>	13	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)	14 (AF13)
15	15	<input type="checkbox"/>	15	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)	16 (CS2)
17	17	<input type="checkbox"/>	17	17
55	55	<input type="checkbox"/>	55	55
56 (CS7)	56 (CS7)	<input type="checkbox"/>	56 (CS7)	56 (CS7)
57	57	<input type="checkbox"/>	57	57
58	58	<input type="checkbox"/>	58	58
59	59	<input type="checkbox"/>	59	59
60	60	<input type="checkbox"/>	60	60
61	61	<input type="checkbox"/>	61	61
62	62	<input type="checkbox"/>	62	62
63	63	<input type="checkbox"/>	63	63

ApplyReset

Figure 3-15.8: The DSCP Translation Configuration

Parameter Description

DSCP: The maximum number of supported DSCP values is 64. The valid DSCP value ranges from 0 to 63.

Ingress: Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation:

1. **Translate:** DSCP at ingress side can be translated to any of (0-63) DSCP values.
2. **Classify:** Click to enable classification at ingress side.

Egress: There are following configurable parameters for egress side –

1. **Remap DP0:** Select the DSCP value from selected menu to which you want to remap. The DSCP value ranges from 0 to 63.
2. **Remap DP1:** Select the DSCP value from selected menu to which you want to remap. The DSCP value ranges from 0 to 63.

There is following configurable parameter for Egress side -

- **Remap:** Select the DSCP value from selected menu to which you want to remap. The DSCP value ranges from 0 to 63.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.9 DSCP Classification

The section teaches the user how to configure and map the DSCP value to a QoS Class and DPL value. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

- a. Click Configuration, QoS, and DSCP Translation.
- b. Scroll to set the DSCP parameters.
- c. Click “Apply” to save the setting.
- d. If you want to cancel the setting, click the reset button to revert back to previously saved values.

DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Apply

Reset

Figure 3-15.9: The DSCP Classification Configuration

Parameter Description

QoS Class: Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.

DPL: Drop Precedence level (0-1) can be configured for all available QoS classes.

DSCP: Select the DSCP value (0-63) from the DSCP menu to map DSCP to corresponding QoS Class and DPL value.

Buttons:


- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.10 QoS Control List Configuration

The section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

- 1. Click Configuration, QoS, and QoS Control List.
- 2. Click the  to add a new QoS Control List.
- 3. Scroll all parameters and evoke the port member to join the QCE rules.
- 4. Click “Apply” to save the setting.
- e. If you want to cancel the setting, click the reset button to revert back to previously saved values.

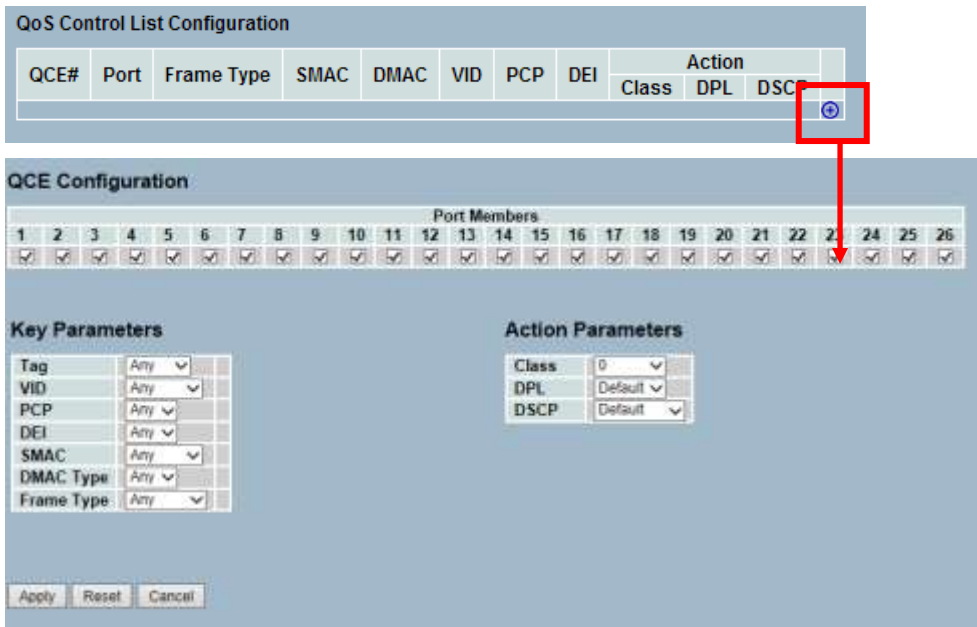


Figure 3-15.10: The QoS Control List Configuration

Parameter Description

- QCE#:** Indicates the index of QCE
- Port:** Indicates the list of ports configured with the QCE.
- Frame Type:** Indicates the type of frame to look for incoming frames. Possible frame types are:
- 1. **Any:** The QCE will match all frame type.
 - 2. **Ethernet:** Only Ethernet frames (with EtherType 0x600-0xFFFF) are allowed.
 - 3. **LLC:** Only (LLC) frames are allowed.
 - 4. **SNAP:** Only (SNAP) frames are allowed
 - 5. **IPv4:** The QCE will match only IPV4 frames.
 - 6. **IPv6:** The QCE will match only IPV6 frames.

SMAC: Displays the OUI field of source MAC address (e.g. first three octet (byte) of MAC address).

DMAC: Specifies the type of destination MAC addresses for incoming frame.

Possible values are:

1. **Any:** All types of destination MAC addresses are allowed.
2. **Unicast:** Only unicast MAC addresses are allowed.
3. **Multicast:** Only multicast MAC addresses are allowed.
4. **Broadcast:** Only broadcast MAC addresses are allowed.
5. The default value is "Any".

VID: Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or "Any".

PCP: Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or "Any".

DEI: Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1, or "Any".

Conflict: Displays QCE status. Resources required to add a QCE may not available. In that case, it shows the conflict status as "Yes". Otherwise, it is always "No". Please note that conflicts can be resolved by releasing the resource required by the QCE and pressing "Refresh" button.

Action: Indicates the classification action taken on the ingress frame if the parameters configured matched the frame's content. There are three action fields: Class, DPL, and DSCP.

1. **Class:** Classified QoS Class; if a frame matches the QCE, it will be put in the queue.
2. **DPL:** Drop Precedence Level; if a frame matches the QCE, then the DP level will set to value displayed under DPL column.
3. **DSCP:** If a frame matches the QCE, then the DSCP will be classified with the value displayed under DSCP column.

Modification Buttons: You can modify each QCE (QoS Control Entry) in the table using the following buttons:



: Inserts a new QCE before the current row.



: Edits the QCE.



: Moves the QCE up the list.



: Moves the QCE down the list.



: Deletes the QCE.



: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members: Mark the checkbox button if you want to make any port a member of the QCL entry. By default, all ports will be checked.

Key Parameters: Key configuration is described as below:

- Tag value of tag field can be “Any”, “Un-tag”, or “Tag”.
- VID valid value of VLAN ID can be in the range of 1-4095 or “Any”. The user can enter either a specific value or a range of VIDs.
- PCP Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or “Any”.
- DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1, or “Any”.
- SMAC Source MAC address: 24 MS bits (OUI) or “Any”.
- DMAC destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC), or “Any”.
- Frame types can be any of the following values:
 - Any
 - Ethernet
 - LLC
 - SNAP
 - IPv4
 - IPv6



NOTE: All frame types are explained below:

1. Any: Allow all types of frames.

2. Ethernet: Valid Ethernet type can have value within 0x600-0xFFFF or “Any”. The default value is “Any”.

3. LLC: SSAP address valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.

DSAP Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.

Control Address Valid Control Address can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.

4. SNAP: PID Valid PID (a.k.a Ethernet type) can have value within 0x00-0xFFFF or “Any”. The default value is “Any”.

5. IPv4: Protocol IP protocol number: (0-255, TCP or UDP) or “Any” Source IP Specific address in value/mask format or “Any”. IP and Mask are in the format x.y.z.w - where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero DSCP Diffserv Code Point value (DSCP). It can be specific value, range of value, or “Any”. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, or AF11-AF43 IP Fragment IPv4 frame fragmented option: yes|no|any.

Sport Source TCP/UDP port: (0-65535) or “Any”. Specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port: (0-65535) or “Any”. Specific or port range applicable for IP protocol UDP/TCP.

6. IPv6: Protocol IP protocol number: (0-255, TCP or UDP) or “Any”.

Source IP IPv6 source address: (a.b.c.d) or “Any”, 32 LS bits.

DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values, or “Any”. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, or AF11-AF43.

Sport Source TCP/UDP port: (0-65535) or “Any”. Specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port: (0-65535) or “Any”. Specific or port range applicable for IP protocol UDP/TCP.

Action Parameters:

- **Class QoS Class:** Class 0-7, default- basic classification.
- DP Valid DP Level can be 0-3, default- basic classification.
- DSCP Valid can be 0-63, BE, CS1-CS7, EF, or AF11-AF43.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-15.11 QCL Status

The section configures and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Configuration, QoS, and QCL Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Scroll to select the combined, static, Voice VLAN, and conflict.
4. Click "Refresh" to refresh an entry of the MVR statistics information.

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DP	DSCP	
Static	2	Any	2-4, 7, 8, 10A-10B	Class 2	Default	Default	No
Static	1	Any	5-10B	Class 0	Default	Default	No

Figure 3-15.11: The QoS Control List Status

Parameter Description

User: Indicates the QCL user.

QCE#: Indicates the index of QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

- **Any:** The QCE will match all frame type.
- **Ethernet:** Only Ethernet frames (with EtherType 0x600-0xFFFF) are allowed.
- **LLC:** Only (LLC) frames are allowed.
- **LLC:** Only (SNAP) frames are allowed.
- **IPv4:** The QCE will match only IPV4 frames.
- **IPv6:** The QCE will match only IPV6 frames.

Port: Indicates the list of ports configured with the QCE.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL, and DSCP.

- **Class:** Classified QoS Class; if a frame matches the QCE, it will be put in the queue.
- **DPL:** Drop Precedence Level; if a frame matches the QCE, then the DP level will set to value displayed under DPL column.
- **DSCP:** If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.

Conflict: Displays the QCE status. Resources required to add a QCE may not be available. In that case, it shows conflict status as “Yes”. Otherwise, it is always “No”. Please note that conflicts can be resolved by releasing the resource required by the QCE and pressing “Refresh” button.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Resolve Conflict: Click to resolve the conflict issue.

Upper right icon (Refresh): You can click them to refresh the QCL information manually.

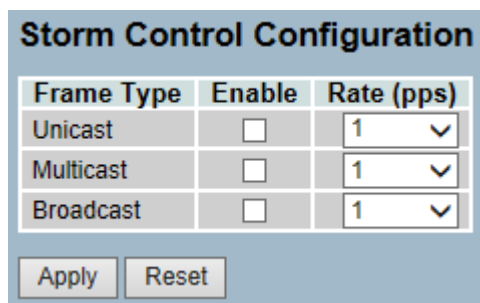
3-15.12 Storm Control

The section configures the storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames (e.g. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table). The configuration indicates the permitted packet rate for the unicast, multicast, or broadcast traffic across the switch.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, and Storm Control Configuration.
2. Evoke to select the frame type to enable storm control.
3. Scroll to set the rate parameters.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.



Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Apply Reset

Figure 3-15.12: The Storm Control Configuration

Parameter Description

Frame Type: The settings in a particular row apply to the frame type listed here: Unicast, Multicast, or Broadcast.

Enable: Enables or disables the storm control status for the given frame type.

Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.

The 1 kpps is actually 1002.1 pps.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**– Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-16 S-Flow Agent

The sFlow Collector configuration for the switch can be monitored and modified here. Up to 1 Collector is supported. This page allows for configuring sFlow collector IP type, sFlow collector IP Address, Port Number, and for each sFlow Collector.

3-16.1 Collector

The "Current" field displays the currently configured sFlow Collector. The "Configured" field displays the new collector configuration.

Web Interface

To configure the sFlow Agent in the web interface:

- 1. Click Configuration, sFlow Agent, and Collector.
- 2. Set the parameters.
- 3. Scroll to choose the IP Type - IPv4 or IPv6.
- 4. Click "Apply" to save the setting.
- 5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

sFlow Receiver Configuration

	Configured	Current
Receiver Id	1	1
IP Type	IPV4 ▾	IPv4
IP Address	0.0.0.0	0.0.0.0
Port	6343	6343
Time Out	0	0
Datagram Size	1400	1400

Apply

Reset

Figure 3-16.1: The sFlow Collector Configuration

Parameter
Description

Receiver Id: The "Receiver ID" input fields allow the user to select the receiver ID. Indicates the ID of this particular sFlow Receiver. Currently, only one ID is supported as only one collector is supported.

IP Type: A drop down list to select the type of IP of collector is displayed. By default, IPv4 is the type of collector IP type. You could use IPv4 or IPv6.

IP Address: The address of a reachable IP is to be entered into the text box. This IP is used to monitor the sFlow samples sent by sFlow agent (our switch). By default, the IP is set to 0.0.0.0 and a new entry has to be added to it.

Port: A port to listen to the sFlow Agent has to be configured for the collector. The value of the port number has to be typed into the text box.

The value accepted is within the range of 1-65535. But an appropriate port number not used by other protocols need to be configured. By default, the port's number is 6343.

Time out: It is the duration during which the collector receives samples. Once it is expired, the sampler stops sending the samples. The value is set through the management before it expires. The value accepted is within the range of 0-2147483647. By default, it is set to 0.

Datagram Size: It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.

Buttons:


- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

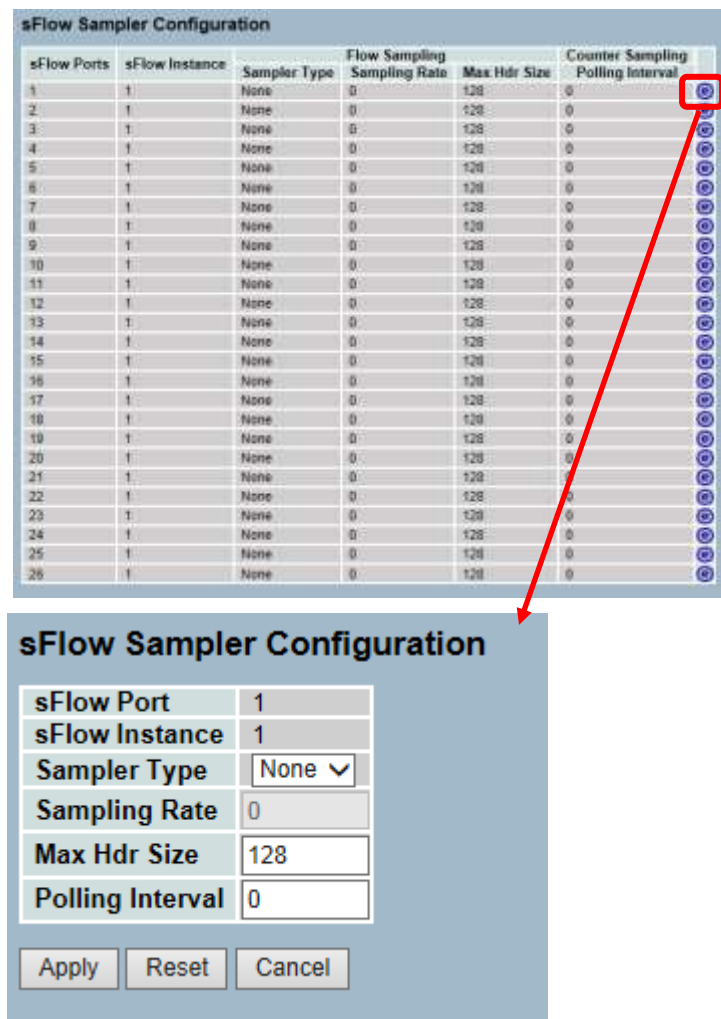
3-16.2 Sampler

The user can set or edit the sFlow sampler for their requirements. That will help the user based on a defined sampling rate. An average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy.

Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow Agent, and sampler.
2. Click the  to edit the sFlow sampler parameters.
3. Scroll to choose the sample type - None, Tx, Rx, or All.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.



The image displays the sFlow Sampler Configuration web interface. It consists of a table listing configurations for various sFlow ports and a detailed configuration form for a selected port.

sFlow Ports	sFlow Instance	Sampler Type	Flow Sampling Sampling Rate	Max Hdr Size	Counter Sampling Polling Interval
1	1	None	0	128	0
2	1	None	0	128	0
3	1	None	0	128	0
4	1	None	0	128	0
5	1	None	0	128	0
6	1	None	0	128	0
7	1	None	0	128	0
8	1	None	0	128	0
9	1	None	0	128	0
10	1	None	0	128	0
11	1	None	0	128	0
12	1	None	0	128	0
13	1	None	0	128	0
14	1	None	0	128	0
15	1	None	0	128	0
16	1	None	0	128	0
17	1	None	0	128	0
18	1	None	0	128	0
19	1	None	0	128	0
20	1	None	0	128	0
21	1	None	0	128	0
22	1	None	0	128	0
23	1	None	0	128	0
24	1	None	0	128	0
25	1	None	0	128	0
26	1	None	0	128	0

The detailed configuration form for sFlow Port 1 shows the following settings:

- sFlow Port: 1
- sFlow Instance: 1
- Sampler Type: None (dropdown menu)
- Sampling Rate: 0
- Max Hdr Size: 128
- Polling Interval: 0

Buttons: Apply, Reset, Cancel

Figure 3-16.2: The sFlow Sampler Configuration

Parameter Description

sFlow Ports: List of the port numbers on which sFlow is configured.

sFlow Instance: Configured sFlow instance for the port number.

Sampler Type: Configured sampler type on the port and could be any of the types: None, Rx, Tx, or All. You can scroll to choose one for your sampler type.


By default, the value is “None”.

Sampling Rate: Configured sampling rate on the ports.

Max Hdr Size: Configured size of the header of the sampled frame.

Polling Interval: Configured polling interval for the counter sampling.

Buttons:

-  - Edits the data source sampler configuration.
- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.
- **Cancel**- Click “Cancel” to cancel to clear up your setting.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the sFlow sampler information manually.

3-17 Loop Protection

3-17.1 Configuration

The loop protection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address, the same as oneself from port, looping happens. The port will be locked when it receives the looping detection frames.

The section describes how to inspect and change the current loop protection configurations.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, and Configuration.
2. Evoke to select enable or disable the port loop protection.
3. Set the parameter and select the action when looping been detected.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

General Settings			
Global Configuration			
Enable Loop Protection	Enable		
Transmission Time	5	seconds	
Shutdown Time	180	seconds	
Port Configuration			
Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable
11	<input checked="" type="checkbox"/>	Shutdown Port	Enable
12	<input checked="" type="checkbox"/>	Shutdown Port	Enable
13	<input checked="" type="checkbox"/>	Shutdown Port	Enable
14	<input checked="" type="checkbox"/>	Shutdown Port	Enable
15	<input checked="" type="checkbox"/>	Shutdown Port	Enable
16	<input checked="" type="checkbox"/>	Shutdown Port	Enable
17	<input checked="" type="checkbox"/>	Shutdown Port	Enable
18	<input checked="" type="checkbox"/>	Shutdown Port	Enable
19	<input checked="" type="checkbox"/>	Shutdown Port	Enable
20	<input checked="" type="checkbox"/>	Shutdown Port	Enable
21	<input checked="" type="checkbox"/>	Shutdown Port	Enable
22	<input checked="" type="checkbox"/>	Shutdown Port	Enable
23	<input checked="" type="checkbox"/>	Shutdown Port	Enable
24	<input checked="" type="checkbox"/>	Shutdown Port	Enable
25	<input checked="" type="checkbox"/>	Shutdown Port	Enable
26	<input checked="" type="checkbox"/>	Shutdown Port	Enable

Apply Reset

Figure 3-17.1: The Loop Protection Configuration

Parameter Description

General Settings

Enable Loop Protection: Controls whether loop protections is enabled (as a whole).

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

Port: The switch port number of the port.

Enable: Controls whether loop protection is enabled on this switch port.

Action: Configures the action performed when a loop is detected on a port. Valid values are shutdown port, shutdown port and log, or log only.

TX Mode: Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-17.2 Status

This page displays the loop protection port status the ports of the switch.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, and Status.
2. Evoke “Auto-refresh” or click “Refresh” to refresh the loop protection port status manually.

Loop Protection Status							Auto-refresh <input type="checkbox"/>	Refresh
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop		
1	Shutdown	Enabled	0	Up	-	-		
2	Shutdown	Enabled	0	Down	-	-		
3	Shutdown	Enabled	0	Down	-	-		
4	Shutdown	Enabled	0	Down	-	-		
5	Shutdown	Enabled	0	Down	-	-		
6	Shutdown	Enabled	0	Down	-	-		
7	Shutdown	Enabled	0	Down	-	-		
8	Shutdown	Enabled	0	Down	-	-		
9	Shutdown	Enabled	0	Down	-	-		
10	Shutdown	Enabled	0	Down	-	-		
11	Shutdown	Enabled	0	Down	-	-		
12	Shutdown	Enabled	0	Down	-	-		
13	Shutdown	Enabled	0	Down	-	-		
14	Shutdown	Enabled	0	Down	-	-		
15	Shutdown	Enabled	0	Down	-	-		
16	Shutdown	Enabled	0	Down	-	-		
17	Shutdown	Enabled	0	Down	-	-		
18	Shutdown	Enabled	0	Down	-	-		
19	Shutdown	Enabled	0	Down	-	-		
20	Shutdown	Enabled	0	Down	-	-		
21	Shutdown	Enabled	0	Down	-	-		
22	Shutdown	Enabled	0	Down	-	-		
23	Shutdown	Enabled	0	Down	-	-		
24	Shutdown	Enabled	0	Down	-	-		
25	Shutdown	Enabled	0	Down	-	-		
26	Shutdown	Enabled	0	Down	-	-		

Figure 3-17.2: The Loop Protection Status.

Parameter Description

Port: The switch port number of the logical port.

Action: The current configured port action.

Transmit: The currently configured port transmit mode.

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port.

Loop: Whether a loop is currently detected on the port.

Time of Last Loop: The time of the last loop event detected.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click this to refresh the loop protection information manually.

3-18 Single IP

Vi3026 provides single IP address management of up to 32 switches and not limited to specific models, distance barriers, specialized cables, or stacking method.

Each single IP group consists of one master switch and up to 32 slave switches. The master switch is used to be an agent to manage all switches in the same group. The slave switch is a switch which wants to join a single IP group, and it could be accessed from the master switch.

3-18.1 Configuration

The section describes how to set the single IP group in this web interface.

Web Interface

To configure the single IP in the web interface:

1. Click Configuration and Single IP.
2. Choose the switch's mode.
3. Giving the group name.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

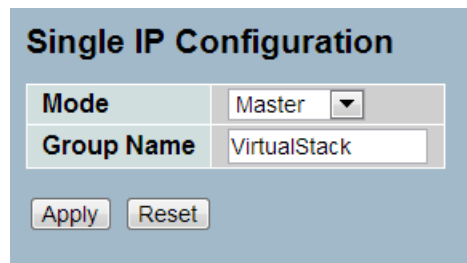


Figure 3-18.1: The Single IP Configuration

Parameter Description

Mode: Possible modes are:

- **Disable:** Disables operation of single IP management.
- **Master:** Enables single IP management and to be a master Switch.
- **Slave:** Enables single IP management and to be a slave Switch.

Group Name: Indicates the name of the single IP group. Maximum length of the group name string is 64.

Buttons:

- **Apply:** Click "Apply" to apply changes.
- **Reset:** Click "Reset" to undo any changes made locally and revert back to previously saved values.

3-18.2 Information

This page displays the active slave switch information.

Web Interface

To display the active slave information in the web interface:

- 1. Click Configuration, Single IP, and Information.
- 2. Evoke "Auto-refresh" or click to refresh the single IP status manually.

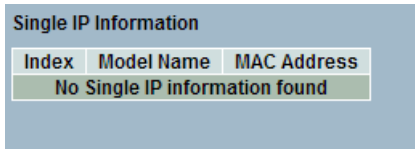


Figure 3-18.2: The Loop Protection Status.

Parameter
Description

Index: The ID of the active slave switch.

Model Name: Displays the model name of the slave switch.

MAC Address: Displays the Ethernet MAC address of the slave switch.

Buttons:

- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.
- **Refresh:** Updates the single IP information.

3-19 Easy Port

Easy Port provides a convenient way to save and share common configurations. You can use it to enable features and settings based on the location of a switch in the network, and for mass configuration deployments across the network. It's easy to implement Voice IP phone, Wireless Access Point, IP Cameras, and more. You can leverage configuration to run a converged voice, video, and data network to consider the quality of service (QoS), bandwidth, latency, and high performance.

Web Interface

To configure the Easy Port in the web interface:

1. Click Configuration and Easy Port.
2. Set the parameters.
3. Scroll the "Role" for what kind device you want to set on the Easy Port and connect to.
4. Click "Apply" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.



NOTE: The easy port configuration page will not actively display the status of setting. The page is for configuring each parameter, so it is correct if the parameter didn't be modified after the selection of each item being applied. The modification will be showed on configuration of individual functionality.

A screenshot of the 'Easy Port Configuration' web interface. At the top, there's a 'Port Members' section with a grid of 26 checkboxes, numbered 1 to 26. Below this is a 'Role' dropdown menu currently set to 'IP-CAM'. A large configuration table follows with various settings: 'Access VLAN' (text input '1'), 'VLAN Mode' (dropdown 'Access'), 'Traffic Class' (dropdown '7'), 'Port Security' (dropdown 'Enable'), 'Port Security Action' (dropdown 'Trap'), 'Port Security Limit' (text input '1'), 'Spanning Tree Admin Edge' (dropdown 'Enable'), and 'Spanning Tree BPDU Guard' (dropdown 'Enable'). At the bottom left of the configuration area are 'Apply' and 'Reset' buttons.

Figure 3-19.1: The Easy Port Configuration

Parameter Description

Port Members: A row of check boxes for each port is displayed for each VLAN ID. To include a port in an Easy Port, check the box as ☒. To remove or exclude the port from the VLAN, make sure the box is unchecked as shown: ☐. By default, no ports are members.

Role: Scroll to select what kind device you want to connect and implement with the Easy Port setting.

Access VLAN: To set the Access VLAN ID means the switch port can access the VLAN ID (AVID).

VLAN Mode: Scroll down to select the VLAN mode with Access, Trunk, or Hybrid.

Traffic Class: Scroll to select the traffic class for the data stream priority. The available value is from 0 (Low) to 7 (High). If you want the voice to have high priority, then you can set the value with 7.

Port Security: Scroll to enable or disable the port security function on the port. If you turn on the function, then you need to set port security limit to allow how many device can access the port (via MAC address).

Port Security Action: Limit control restricts the number of users on a given port. A user is identified by a MAC address and VLAN ID. If limit control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

- **None:** Does not allow more than the limit MAC addresses on the port, but take no further action.
- **Trap:** If limit + 1 MAC address is seen on the port, then it sends a SNMP trap. If aging is disabled, only one SNMP trap will be sent. If aging is enabled, new SNMP traps will be sent every time the limit gets exceeded.
- **Shutdown:** If limit + 1 MAC addresses is seen on the port, it shuts down the port. This implies that all secured MAC addresses will be removed from the port and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
 1. Boots the stack or elect a new master switch.
 2. Disables and re-enables limit control on the port or the stackswitch.
 3. Click the "Reopen" button.
- **Trap & Shutdown:** If limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

Port Security limit: The maximum number of MAC addresses that can be secured. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, a configured maximum may not be granted if the remaining ports have already used all available MAC addresses.

Spanning Tree Admin Edge: Control whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).

Spanning Tree BPDU Guard: If this is enabled, the port will disable itself once it receives the valid BPDU's. Contrary to the similar bridge setting, the port edge status does not affect this setting.

A port entering error-disabled state due to this setting is subject to the bridge port error recovery setting as well.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

3-20 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are monitoring port and monitored port respectively. Thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration and Mirroring.
2. Scroll to select the port to mirror.
3. Scroll to set the port mirror mode: disabled, enable, TX only, and RX only.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Mirror Configuration

Port to mirror to: Disabled ▼

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
10	Disabled ▼
11	Disabled ▼
12	Disabled ▼
13	Disabled ▼
14	Disabled ▼
15	Disabled ▼
16	Disabled ▼
17	Disabled ▼
18	Disabled ▼
19	Disabled ▼
20	Disabled ▼
21	Disabled ▼
22	Disabled ▼
23	Disabled ▼
24	Disabled ▼
25	Disabled ▼
26	Disabled ▼

Apply Reset

Figure 3-21.1: The Mirror Configuration

Parameter Description

Port to mirror: Port to mirror is also known as the mirror port. Frames from ports that have either source (RX) or destination (TX) mirroring enabled are mirrored on this port. "Disabled" will disable mirroring.

Mirroring Port Configuration

The following table is used for RX and TX enabling.

Port: The logical port for the settings contained in the same row.

Mode: Selects mirror mode.

- "RX Only" - Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- "TX Only" - Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
- "Disabled" - Neither frames transmitted or frames received are mirrored.
- "Enabled" - Frames received and frames transmitted are mirrored on the mirror port.



NOTE: For a given port, a frame is only transmitted once. Therefore, it's not possible to mirror TX frames on the mirror port. Because of this, the mode for the selected mirror port is limited to "Disabled" or "Rx Only".

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

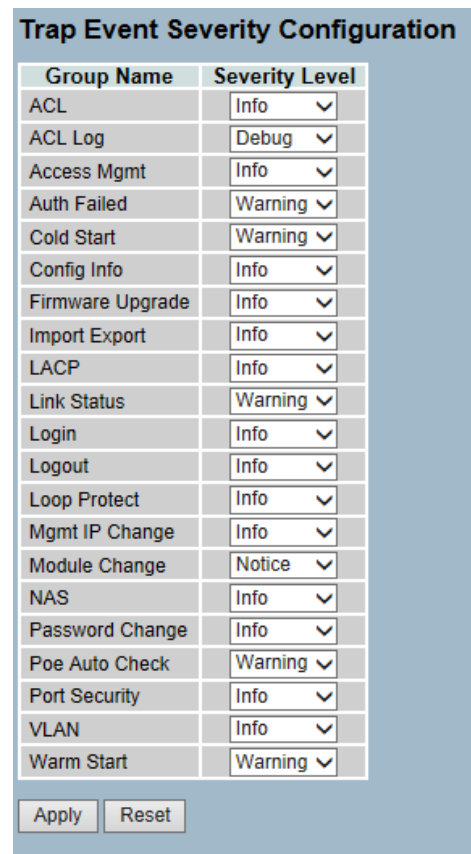
3-21 Trap Event Severity

The function is used to set an alarm trap and get the event log. The trap events configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred.

Web Interface

To configure the Trap Event Severity Configuration in the web interface:

1. Click Configuration and Trap Event Severity Configuration.
2. Scroll to select the group name and severity level.
3. Click “Apply” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.



Group Name	Severity Level
ACL	Info
ACL Log	Debug
Access Mgmt	Info
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Import Export	Info
LACP	Info
Link Status	Warning
Login	Info
Logout	Info
Loop Protect	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Password Change	Info
Poe Auto Check	Warning
Port Security	Info
VLAN	Info
Warm Start	Warning

Apply Reset

Figure 3-21.1: The Trap Event Severity Configuration

Parameter Description

Group Name: The field describes the trap event definition.

Severity Level: Scroll to select the event type - Emerg, Alert, Crit, Error, Warning, Notice, Info, or Debug.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset** - Click “Reset” to undo any changes made locally and revert back to previously saved values.

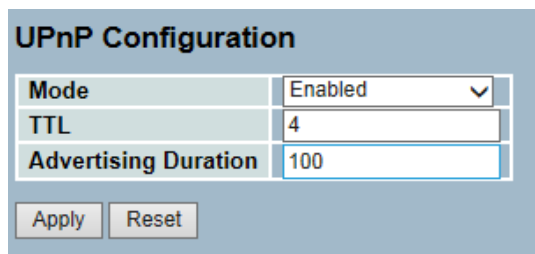
3-22 UPnP

UPnP is an acronym for universal plug and play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration and UPnP.
2. Scroll to select the mode - Enable or Disable.
3. Specify the parameters in each blank field.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.



UPnP Configuration	
Mode	Enabled
TTL	4
Advertising Duration	100
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 3-22.1: The UPnP Configuration

Parameter Description

These parameters are displayed on the UPnP configuration page:

Mode: Indicate the UPnP operation mode. Possible modes are:

- **Enabled:** Enables the UPnP mode operation.
- **Disabled:** Disables the UPnP mode operation.
- When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range of 1 to 255.

Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points on how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard, it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

Chapter 4: Security

4-1 IP Source Guard

4-1.1 Configuration

This chapter describes all of the switch security configuration tasks to enhance the security of local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, and more.

The section describes how to configure the IP source guard detail parameters of the switch. You could use the IP source guard configure to enable or disable with the port of the switch.

This section describes how to configure IP Source Guard setting including:

- Mode (Enabled and Disabled)
- Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Selects “Enabled” in the mode of IP source guard configuration.
2. Selects “Enabled” of the specific port in the mode of port mode configuration.
3. Select maximum dynamic clients (0, 1, 2, Unlimited) of the specific port in the mode of port mode configuration.
4. Click “Apply”.



Figure 4-1.1: The IP Source Guard Configuration

**Parameter
description**

Mode of IP Source Guard Configuration: Enables the global IP source guard or disables the global IP source guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration: Specifies that the IP source guard is enabled on which ports. Only when both global mode and port mode on a given port are enabled, the IP source guard is enabled on this given port.

Max Dynamic Clients: Specifies the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2, or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it only allows the IP packets forwarding that are matched in the static entries on the specific port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-1.2 Static Table

The section describes how to configure the static IP source guard table parameters of the switch. You could configure the static IP source guard table to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click "Add New Entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click "Apply".

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Add new entry				
Apply Reset				

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			
Add new entry				
Apply Reset				

Figure 4-1.2: The Static IP Source Guard Table

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

IP Address: Allowed source IP address.

MAC address: Allowed source MAC address.

Adding new entry: Click to add a new entry to the static IP source guard table. Specifies the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset** – Click "Reset" to undo any changes made locally and revert back to previously saved values.

4-1.3 Dynamic Table

The section configures the dynamic IP source guard table parameters of the switch. You could use the dynamic IP source guard Table configure to manage the entries.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the web interface:

- 1. Specify the start from port, VLAN ID, IP Address, and entries per page.
- 2. Checked "Auto-refresh".

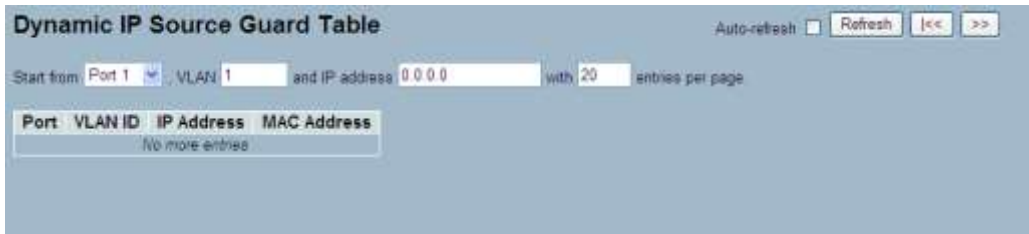


Figure 4-1.3: The Dynamic Table

Parameter Description

- Port:** Switch port number for which the entries are displayed.
- VLAN ID:** VLAN-ID in which the IP traffic is permitted.
- IP Address:** User IP address of the entry.
- MAC Address:** Source MAC address.
- Auto-refresh:** Evoke the auto-refresh icon to refresh the information automatically.
- Upper right icon (Refresh, <<, >>):** You can click them to refresh the Dynamic IP Source Guard Table manually. Click "<<" or ">>" to move to the next or previous page.

4-2 ARP Inspection

The section describes how to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

4-2.1 Configuration

This section describes how to configure the ARP inspection setting including:

- Mode (Enabled and Disabled)
- Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Select “Enabled” in the mode of ARP inspection configuration.
2. Select “Enabled” of the specific port in the mode of port mode configuration.
3. Click “Apply”.

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Apply Reset

Figure 4-2.1: The ARP Inspection Configuration

**Parameter
Description**

Mode of ARP Inspection Configuration: Enables or disables the global ARP inspection.

Port Mode Configuration: Specifies the ARP Inspection is enabled on which ports. Only when both global mode and port mode on a given port are enabled, ARP inspection is enabled on this given port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-2.2 Static Table

The section configures the static ARP inspection table parameters of the switch. You could use the static ARP inspection table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click "Add New Entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click "Apply".

The figure shows two screenshots of the 'Static ARP Inspection Table' web interface. The top screenshot shows the 'Add new entry' button highlighted with a red box and a red arrow pointing to the bottom screenshot. The bottom screenshot shows the table with one entry: Port 1, VLAN ID, MAC Address, and IP Address fields.

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Figure 4-2.2: The Static ARP Inspection Table

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

MAC Address: Allowed source MAC address in ARP request packets.

IP Address: Allowed source IP address in ARP request packets.

Adding new entry: Click to add a new entry to the static ARP inspection table. Specifies the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save".

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset** – Click "Reset" to undo any changes made locally and revert back to previously saved values.

4-2.3 Dynamic Table

The section configures the dynamic ARP inspection table parameters of the switch. The dynamic ARP inspection table contains up to 1024 entries and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

- To configure a Dynamic ARP Inspection Table Configuration in the web interface:
1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.
 2. Checked "Auto-refresh".



Figure 4-2.3: The Dynamic ARP Inspection Table

Parameter Description

- Port:** Switch port number for which the entries are displayed.
- VLAN ID:** VLAN-ID in which the ARP traffic is permitted.
- MAC Address:** User MAC address of the entry.
- IP Address:** User IP address of the entry.
- Auto-refresh:** Evoke the auto-refresh icon to refresh the information automatically.
- Upper right icon (Refresh, <<, >>):** You can click them to refresh the Dynamic ARP Inspection Table manually. Click "<<" or ">>" to move to the next or previous page.

4-3 DHCP Snooping

The section describes how to configure the DHCP snooping parameters of the switch. The DHCP snooping can prevent attackers from adding their own DHCP servers to the network.

4-3.1 Configuration

This section describes how to configure DHCP snooping setting including:

- Snooping Mode (Enabled and Disabled)
- Port Mode Configuration (Trusted, Untrusted)

Web Interface

To configure a DHCP Snooping in the web interface:

1. Select “Enabled” in the mode of DHCP snooping configuration.
2. Select “Trusted” of the specific port in the mode of port mode configuration.
3. Click “Apply”.

DHCP Snooping Configuration

Snooping Mode: Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
9	Untrusted
10	Untrusted
11	Untrusted
12	Untrusted
13	Untrusted
14	Untrusted
15	Untrusted
16	Untrusted
17	Untrusted
18	Untrusted
19	Untrusted
20	Untrusted
21	Untrusted
22	Untrusted
23	Untrusted
24	Untrusted
25	Untrusted
26	Untrusted

Apply Reset

Figure 4-3.1: The DHCP Snooping Configuration

**Parameter
Description**

Snooping Mode: Indicates the DHCP snooping mode operation. Possible modes are:

- **Enabled:** Enables DHCP snooping mode operation. When the DHCP snooping mode operation is enabled, the DHCP requests messages to be forwarded to trusted ports and only allow reply packets from trusted ports.
- **Disabled:** Disable the DHCP snooping mode operation.

Port Mode: Indicates the DHCP snooping port mode. Possible port modes are:

- **Trusted:** Configures the port as trusted source of the DHCP messages.
- **Untrusted:** Configures the port as untrusted source of the DHCP messages.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-3.2 Statistics

The section describes how to show the DHCP snooping statistics information of the switch. The statistics show only packet counters when the DHCP snooping mode is enabled and the relay mode is disabled. It doesn't count the DHCP packets for the DHCP client.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:

- 1. Specify the port that you want to monitor.
- 2. Checked "Auto-refresh".

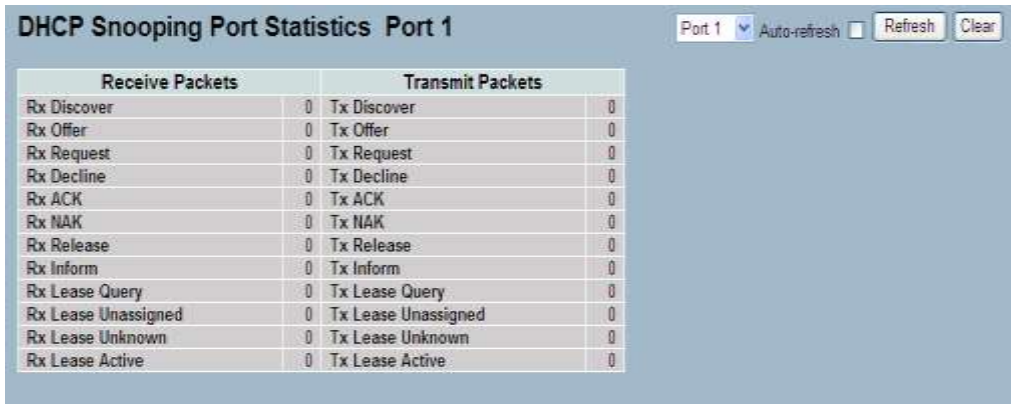


Figure 4-3.2: The DHCP Snooping Port Statistics

Parameter Description

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear): You can click them to refresh the DHCP snooping port statistics manually. Click “Clear” to clean up the entries.

4-4 DHCP Relay

The section describes how to forward the DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

4-4.1 Configuration

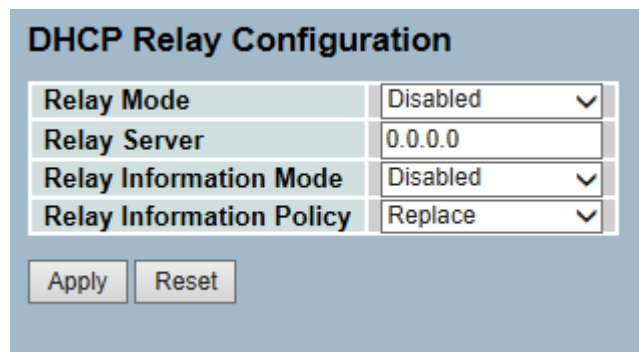
This section describes how to configure DHCP relay setting including:

- Relay Mode (Enabled and Disabled)
- Relay Server IP setting
- Relay Information Mode (Enabled and Disabled)
- Relay Information Mode Policy (Replace, Keep and Drop)

Web Interface

To configure a DHCP Relay in the web interface:

1. Select “Enabled” in the relay mode of DHCP relay configuration.
2. Specify “Relay Server IP” address.
3. Select “Enabled” in the relay information mode of dhcp relay configuration.
4. Specify “Relay” (Replace, Keep and Drop) in the relay information mode of DHCP relay configuration.
5. Click “Apply”.



DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 4-4.1: The DHCP Relay Statistics

Parameter Description

Relay Mode: Indicates the DHCP relay mode operation. Possible modes are:

- **Enabled:** Enables DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers the DHCP messages between the clients and the server when they are not in the same subnet domain. The DHCP broadcast message won't be flooded for security considerations.
- **Disabled:** Disables the DHCP relay mode operation.

Relay Server: Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer the DHCP messages between the clients and the server when they are not in the same subnet domain.

Relay Information Mode: Indicates the DHCP relay information mode operation. Possible modes are:

- **Enabled:** Enables the DHCP relay information mode operation. When the DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removing it from a DHCP message when transferring to

DHCP client. It only works when DHCP relay operation mode is enabled.

- **Disabled:** Disables the DHCP relay information mode operation.

Relay Information Policy: Indicates the DHCP relay information option policy. When the DHCP relay information mode operation is enabled and if the agent receives a DHCP message that already contains the relay agent information, it will enforce the policy. It only works under DHCP if the relay information operation mode is enabled. Possible policies are:

- **Replace:** Replaces the original relay information when a DHCP message that already contains is received.
- **Keep:** Keeps the original relay information when a DHCP message that already contains is received.
- **Drop:** Drops the package when a DHCP message that already contains relay information is received.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-4.2 Statistics

The section describes how to show the DHCP relay statistics information of the switch. The statistics shows both the server and the client packet counters when the DHCP relay mode is enabled.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:

1. Checked "Auto-refresh".

Server Statistics							
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Figure 4-4.2: The DHCP Relay Statistics

Parameter Description

Transmit to Server: The number of packets that are relayed from the client to the server.

Transmit Error: The number of packets that resulted in errors while being sent to the clients.

Receive from Server: The number of packets received from the server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the "Circuit ID" option missing.

Receive Missing Remote ID: The number of packets received with the "Remote ID" option missing.

Receive Bad Circuit ID: The number of packets whose "Circuit ID" option did not match known "Circuit ID".

Receive Bad Remote ID: The number of packets whose "Remote ID" option did not match known "Remote ID".

Clients Statistics

Transmit to Client: The number of relayed packets from the server to the client.

Transmit Error: The number of packets that resulted in error while being sent to the servers.

Receive from Client: The number of received packets from the server.

Receive Agent Option: The number of received packets with the relay agent information option.

Replace Agent Option: The number of packets which were replaced with the relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped, which were received with relay agent information.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear): You can click them to refresh the DHCP relay statistics manually. Click “Clear” to clean up the entries.

4-5 NAS

The section describes how configure the NAS parameters of the switch. The NAS server can be employed to connect users to a variety of resources including internet access, conference calls, printing documents on shared printers, or by simply logging on to the internet.

4-5.1 Configuration

This section describes how to configure NAS setting of IEEE 802.1X, MAC-based authentication system, and port settings. The NAS configuration consists of two sections, a system-wide and a port-wide.

Web Interface

To configure a System Configuration of Network Access Server in the web interface:

1. Select “Enabled” in the mode of network access server configuration.
2. Checked “Reauthentication Enabled”.
3. Set “Reauthentication Period”. The default is 3600 seconds.
4. Set “EAPOL Timeout”. The default is 30 seconds.
5. Set “Aging Period”. The default is 300 seconds.
6. Set “Hold Time”. The default is 10 seconds.
7. Checked “RADIUS-Assigned QoS Enabled”.
8. Checked “RADIUS-Assigned VLAN Enabled”.
9. Checked “Guest VLAN Enabled”.
10. Specify the guest VLAN ID.
11. Specify Max. Reauth. count.
12. Checked “Allow Guest VLAN if EAPOL Seen”.
13. Click “Apply”.

Network Access Server Configuration

System Configuration

Mode:

Reauthentication Enabled: ☒

Reauthentication Period: seconds

EAPOL Timeout: seconds

Aging Period: seconds

Hold Time: seconds

RADIUS-Assigned QoS Enabled: ☒

RADIUS-Assigned VLAN Enabled: ☒

Guest VLAN Enabled: ☒

Guest VLAN ID:

Max. Reauth. Count:

Allow Guest VLAN if EAPOL Seen: ☒

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Revert
1	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
2	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
3	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
4	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
5	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
6	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
7	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
8	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
9	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
10	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
11	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
12	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
13	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
14	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
15	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
16	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
17	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
18	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
19	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
20	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
21	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
22	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
23	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication
24	Force Authorized	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthentication

Apply Revert

Figure 4-5.1: The Network Access Server Configuration

Parameter Description

Mode: Indicates if the NAS is globally enabled or disabled on the switch. If the NAS is globally disabled, all ports are allowed to forward frames.

Reauthentication Enabled: If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the reauthentication period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. If it does not involve communication between the switch and the client, therefore it doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period: Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if "Reauthentication Enabled" is checked. The valid values are in the range 1 to 3600 seconds.

EAPOL Timeout: Determines the time for retransmission of request identity EAPOL frames. The valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

Aging Period: This setting applies to the following modes (e.g. modes using the port security functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the port security module to secure the MAC addresses, the port security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If the reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical since the supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time: This setting applies to the following modes (e.g. modes using the Port Security functionality to secure MAC addresses):

- **Single 802.1X**
- **Multi 802.1X**
- **MAC-Based Auth.**

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The hold time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled: The RADIUS-assigned QoS provides a mean to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable the RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether the RADIUS-assigned QoS class is enabled on that port. When unchecked, the RADIUS-server assigned QoS class is disabled on all ports.

RADIUS –Assigned VLAN Enabled: The RADIUS-assigned VLAN provides a mean to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable the RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether the RADIUS-assigned VLAN is enabled on that port. When unchecked, the RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A guest VLAN is a special VLAN (typically with limited network access) that 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable the Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into guest VLAN. When unchecked, the ability to move to the guest VLAN is disabled on all ports.

Guest VLAN ID: This is the value that a port's "Port VLAN ID" is set to if a port is moved to the guest VLAN. It is only changeable if the "Guest VLAN" option is globally enabled. The valid values are in the range of 1- 4095.

Max Reauth. Count: The number of times the switch transmits an EAPOL request identity frame without response before entering the Guest VLAN. The value can only be changed if the "Guest VLAN" option is globally enabled. The valid values are in the range of 1-255.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Port: The port number for which the configuration below applies.

Admin State: If the NAS is globally enabled, “Admin State” controls the port's authentication mode. The following modes are available:

- **Forced Authorized:** In this mode, the switch will send one EAPOL success frame when the port link comes up. Any client on the port will be allowed network access without authentication.
- **Forced Unauthorized:** In this mode, the switch will send one EAPOL failure frame when the port link comes up. Any client on the port will be disallowed network access.
- **Port-Based 802.1X:** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the middleman. The authenticator forwards requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are the RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes (switch's IP address, name, and the supplicant's port number) on the switch. EAP allows different authentication methods (MD5-Challenge, PEAP, and TLS). The authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet that contains a success or failure indication. Aside from forwarding this decision to the supplicant, the switch also uses it to open or block traffic on the switch port connected to the supplicant.



NOTE: Supposed two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and that the first server in the list is currently down (but not considered dead).

Now, if the supplicant retransmits the EAPOL start frames at a rate faster than X seconds, then it will never get authenticated because the switch will cancel the on-going backend authentication server requests whenever it receives a new EAPOL start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL start frame retransmission rate.

Single 802.1X: Once a supplicant is successfully authenticated on a port in a port-based 802.1X authentication, the whole port is opened for network traffic. This allows other clients connected to the port (e.g. through a hub) to piggy-back on the successfully authenticated client and get network access, even though they really aren't authenticated. To overcome this security breach, use the single 802.1X variant. The single 802.1X is really not an IEEE standard, but features many of the same characteristics as the port-based 802.1X. In the single 802.1X, only one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used to communicate between the supplicant and the switch. If more than one supplicant is connected to a port, the first one that comes when the port's link comes up will be considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the port security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: Once a supplicant is successfully authenticated on a port in a port-based 802.1X authentication, the whole port is opened for network traffic. This allows other clients connected to the port (e.g. through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as the port-based 802.1X. With multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table by using the port security module.

In Multi 802.1X, it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch towards the supplicant since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception is when no supplicants are attached. In this case, the switch sends EAPOL request identity frames using the BPDU multicast MAC address as destination to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the port security limit control functionality.

MAC-Based Auth: Unlike the port-based 802.1X, the MAC-based authentication is not a standard. It's only a best-practices method adopted by the industry. In MAC-based authentication, users are called clients and the switch acts as the supplicant on behalf of the clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx". A dash (-) is used as a separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When the authentication is complete, the RADIUS server sends a success or failure indication. It will cause the switch to open or block traffic for that particular client using the port security module.

Only then, will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication. Therefore, the MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of the MAC-based authentication over the port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication. The clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled: When the RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If it's present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS class is immediately reverted to the original QoS class. This may be changed by the administrator without affecting the RADIUS-assigned. This option is only available for single-client modes.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range 0-3, which translates into the desired QoS Class in the range of 0-3.

RADIUS-Assigned VLAN Enabled: When the RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If it's present and valid, the port's "Port VLAN ID" will be changed to this VLAN ID. The port will be set to be a member of that VLAN ID and will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator without affecting the RADIUS-assigned). This option is only available for single-client modes.

- Port-based 802.1X
- Single 802.1X

To trouble-shoot the VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range 0-9, which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled: When the guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

To trouble-shoot the VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation: When a guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL request identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received, the switch will consider entering the guest VLAN. The interval between transmissions of EAPOL request identity frames is configured with EAPOL timeout. If "Allow Guest VLAN if EAPOL Seen" is enabled, the port will now be placed in the guest VLAN. If it's disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port. This history is cleared if the port link goes down or the port's Admin State is changed. If not, the port will be placed in the guest VLAN. Otherwise, it will not move to the guest VLAN, but continue transmitting EAPOL request identity frames at the rate given by EAPOL timeout.

Once in the guest VLAN, the port is considered authenticated and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL success frame when entering the guest VLAN.

While in the guest VLAN, the switch monitors the link for EAPOL frames and if one such frame is received, the switch immediately takes the port out of the guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State: The current state of the port. It can undertake one of the following values:

- **Globally Disabled:** NAS is globally disabled.
- **Link Down:** NAS is globally enabled, but there is no link on the port.
- **Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart: Two buttons are available for each row. The buttons are only enabled when the authentication is globally enabled and the port's admin state is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.
- The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

Upper right icon (Refresh): You can click them to refresh the NAS Configuration manually.

4-5.2 Switch Status

The section shows the NAS status information of each port on the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the web interface:

- 1. Checked "Auto-refresh".

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				

Figure 4-5.2: The Network Access Server Switch Status

Parameter Description

- Port:** The switch port number. Click to navigate to detailed NAS statistics for this port.
- Admin State:** The port's current administrative state. Refer to NAS Admin State for a description of possible values.
- Port State:** The current state of the port. Refer to NAS Port State for a description of the individual states.
- Last Source:** The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
- Last ID:** The user name (supplicant identity) carried in the most recently received response identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
- QoS Class:** QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank, if the port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the guest VLAN, "(Guest)" is appended to the VLAN ID.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the NAS switch status manually.

4-5.3 Port Status

The section provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the web interface:

- 1. Specify the port you want to check.
- 2. Checked "Auto-refresh".



Figure 4-5.3: The NAS Port Statistics

Parameter Description

Port State

Admin State: The port's current administrative state. Refer to NAS admin state for a description of possible values.

Port State: The current state of the port. Refer to NAS port state for a description of the individual states.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear): You can click them to refresh the NAS statistics manually. Click "Clear" to clean up all entries.

4-6 AAA

This section uses an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

4-6.1 Configuration

This section configures the AAA setting of the TACACS+ or RADIUS server.

Web Interface

To configure a common configuration of AAA in the web interface:

1. Set "Timeout". The default is 15 seconds.
2. Set "Dead Time". The default is 300 seconds.

To configure a TACACS+ authorization and accounting configuration of AAA in the web interface:

1. Select "Enabled" in the Authorization.
2. Select "Enabled" in the Failback to Local Authorization.
3. Select "Enabled" in the Account.

To configure a RADIUS authentication server configuration of AAA in the web interface:

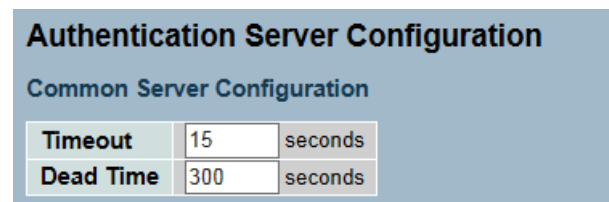
1. Check "Enabled".
2. Specify IP address or hostname for the radius server.
3. Specify authentication port for the radius server. The default is 1812.
4. Specify the "Secret" with radius server.

To configure a RADIUS accounting server configuration of AAA in the web interface:

1. Check "Enabled".
2. Specify IP address or hostname for the radius server.
3. Specify accounting port for the radius server. The default is 1813.
4. Specify the "secret" with the radius server.

To configure a TACACS+ authentication server configuration of AAA in the web interface:

1. Check "Enabled".
2. Specify IP address or hostname for the TACACS+ server.
3. Specify authentication port for the TACACS+ server. The default is 49.
4. Specify the "Secret" with the TACACS+ server.



The screenshot shows a web interface titled "Authentication Server Configuration". Under the "Common Server Configuration" section, there are two rows of configuration fields. The first row is for "Timeout", with a text input field containing "15" and a dropdown menu set to "seconds". The second row is for "Dead Time", with a text input field containing "300" and a dropdown menu set to "seconds".

Authentication Server Configuration		
Common Server Configuration		
Timeout	15	seconds
Dead Time	300	seconds

Figure 4-5.3.1: The Common Server Configuration

TACACS+ Authorization and Accounting Configuration

Authorization	Disabled ▾
Fallback to Local Authorization	Disabled ▾
Accounting	Disabled ▾

Figure 4-5.3.2: The TACACS+ Accounting Configuration

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

Figure 4-5.3.3: The RADIUS Configuration

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

Figure 4-5.3.4: The RADIUS Accounting Configuration

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

Figure 4-5.3.5: The TACACS+ Authentication Configuration

Parameter Description

Timeout: Timeout is the maximum time to wait for a reply from a server. It can be set to a number between 3 and 3600 seconds.

If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

The RADIUS servers are using the UDP protocol. It is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time: Dead Time is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. It can be set to a number between 0 and 3600 seconds. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the dead time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

Authorization: Every CLI commands will be authorized by the TACACS+ server when it's enabled. The authorization table on the TACACS+ server is able to configure which CLI command can pass successfully. For example, the TACACS+ server is set to accept the STP command but deny the VLAN command. The server will block the command related to the STP which is entered by user, but it can allow the VLAN command to configure successfully when user enters the VLAN command.

Fallback to Local Authorization: Enabled to allow the user who typed the wrong account or password to login successfully when the user account is on the local authorization list of the local switch. For example, when the user entered the wrong account or password, the TACACS+ server will refer to the account information on the local end of switch. If the account is recorded on the local switch, the user will be authorized to login with the privilege level set on the local switch.

Accounting: Enabled to record all the commands that the user entered. All the log data will be recorded on the server when it's enabled. For instance, login time, log out time, IGMP setting, VLAN setting, etc.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS authentication server and a number of columns, which are:

#: The RADIUS authentication server number for which the configuration below applies.

Enabled: Enables the RADIUS authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS authentication server. The IP address is expressed in dotted decimal notation.

Port: The UDP port used on the RADIUS authentication server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS authentication server.

Secret: The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS accounting server and a number of columns, which are:

#: The RADIUS accounting server number for which the configuration below applies.

Enabled: Enable the RADIUS accounting server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.

Port: The UDP port to use on the RADIUS accounting server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS accounting server.

Secret: The secret - up to 29 characters long - shared between the RADIUS accounting server and the switch stack.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ authentication server and a number of columns, which are:

#: The TACACS+ authentication server number for which the configuration below applies.

Enabled: Enables the TACACS+ authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the TACACS+ authentication server. The IP address is expressed in dotted decimal notation.

Port: The TCP port used on the TACACS+ authentication server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ authentication server.

Secret: The secret - up to 29 characters long - shared between the TACACS+ authentication server and the switch stack.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-6.2 Radius Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

Web Interface

To configure a RADIUS Overview Configuration in the web interface:

- 1. Checked "Auto-refresh".

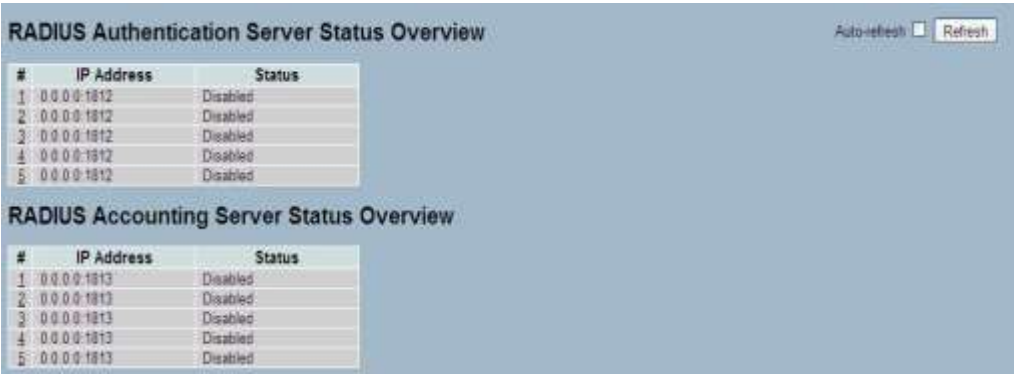


Figure 4-6.2: The RADIUS Authentication Server Status Overview

Parameter Description

#: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State: The current state of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but the IP communication is not yet up and running.
- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- **Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

#: The RADIUS server number. Click to navigate the detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State: The current state of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but the IP communication is not yet up and running.
- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- **Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the RADIUS status manually.

4-6.3 Radius
Details

This section shows the detailed statistics of the RADIUS authentication and accounting servers. The statistics mapped closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS Details Configuration in the web interface:

- 1. Specify the port that you want to check.
- 2. Checked "Auto-refresh".

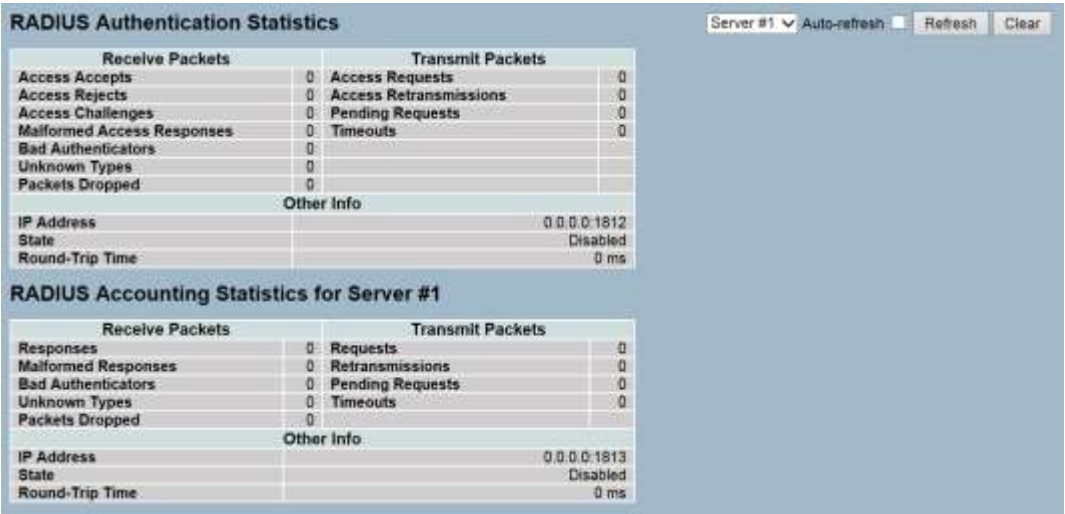


Figure 4-6.3: The RADIUS Authentication Statistics Server

Parameter
Description

RADIUS Authentication Statistics

The statistics mapped closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or message authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a request, as well as, a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.
------------------------	----------------------------------	--

RADIUS

Accounting Statistics

The statistics mapped closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the

			same server is counted as a retransmission and a timeout. A send to a different server is counted as a request and a timeout.
--	--	--	---

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons:

- **Auto-refresh** –Check to automatically refresh at regular intervals.
- **Refresh** - Click to refresh the page immediately.
- **Clear** - Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4-7 Port Security

4-7.1 Limit Control

This section configures the port security settings of the switch. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses.

This section configures the port security settings of the switch. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a System Configuration of Limit Control in the web interface:

1. Select “Enabled” in the Mode of System Configuration.
2. Checked “Aging Enabled”.
3. Set “Aging Period”. The default is 3600 seconds.

To configure a Port Configuration of Limit Control in the web interface:

1. Select “Enabled” in the mode of port configuration.
2. Specify the maximum number of MAC addresses in the limit of port configuration.
3. Set “Action” (Trap, Shutdown, Trap & Shutdown).
4. Click “Apply”.

Port	Mode	Limit	Action	State	Re-open
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen

Figure 4-7.1: The Port Security Limit Control Configuration

Parameter Description

System Configuration

Mode: Indicates if the limit control is globally enabled or disabled on the switch. If it's globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled: If this is checked, secured MAC addresses are subject to aging as discussed under "Aging Period".

Aging Period: If "Aging Enabled" is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements for the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The "Aging Period" can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Supposed an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which limit control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next aging period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Port: The port number to which the configuration below applies.

Mode: Controls whether the limit control is enabled on this port. Both this and the global mode must be set to enabled for limit control to be in effect. Notice that other modules may still use the underlying port security features without enabling limit control on a given port.

Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action: If Limit is reached, the switch can take one of the following actions:

- **None:** Do not allow more than Limit MAC addresses on the port, but take no further action.
- **Trap:** If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
- **Shutdown:** If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the

port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1. Boot the switch,
 2. Disable and re-enable Limit Control on the port or the switch,
 3. Click the Reopen button.
- **Trap & Shutdown:** If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State: This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- **Disabled:** Limit Control is either globally disabled or disabled on the port.
- **Ready:** The limit is not yet reached. This can be shown for all actions.
- **Limit Reached:** Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- **Shutdown:** Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shut down or Trap & Shutdown.

Re-open Button: If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shut down in the Action section.



NOTE: That clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

Upper right icon (Refresh): You can click them to refresh the Port Security information manually.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset**- Click "Reset" to undo any changes made locally and revert back to previously saved values.

4-7.2 Switch Status

This section shows the port security status. Port security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed onto the port security module, which in turn asked all user modules whether to allow or block this new MAC address from forwarding. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agreed on allowing the MAC address to forward. If one chose to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Checked "Auto-refresh"

Port Security Switch Status

Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	S
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	0	0
2	----	Disabled	0	0
3	----	Disabled	0	0
4	----	Disabled	0	0
5	----	Disabled	0	0
6	----	Disabled	0	0
7	----	Disabled	0	0
8	----	Disabled	0	0
9	----	Disabled	0	0
10	----	Disabled	0	0
11	----	Disabled	0	0
12	----	Disabled	0	0
13	----	Disabled	0	0
14	----	Disabled	0	0
15	----	Disabled	0	0
16	----	Disabled	0	0
17	----	Disabled	0	0
18	----	Disabled	0	0
19	----	Disabled	0	0
20	----	Disabled	0	0
21	----	Disabled	0	0
22	----	Disabled	0	0
23	----	Disabled	0	0
24	----	Disabled	0	0
25	----	Disabled	0	0
26	----	Disabled	0	0

Figure 4-7.2: The Port Security Switch Status

Parameter Description

User Module Legend

The legend shows all user modules that may request port security services.

User Module Name: The full name of a module that may request port security services.

Abbr: A one-letter abbreviation of the user module. This is used in the “Users” column in the port status table.

Port Status

The table has one row for each port on the selected switch and a number of columns, which are:

Port: The port number for which the status applies. Click the port number to see the status for this particular port.

Users: Each of the user modules has a column that shows whether or not port security is enabled. A “-” means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State: Shows the current state of the port. It can take one of four values:

- **Disabled:** No user modules are currently using the port security service.
- **Ready:** The port security service is in use by at least one user module, and is waiting for frames from unknown MAC addresses to arrive.
- **Limit Reached:** The port security service is enabled by at least the limit control user module. That module has indicated that the limit is reached and no more MAC addresses should be taken in.
- **Shutdown:** The port security service is enabled by at least the limit control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively reopened on the limit control configuration web-page.

MAC Count (Current, Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

- If no user modules are enabled on the port, the “Current” column will show a dash (-).
- If the limit control user module is not enabled on the port, the “Limit” column will show a dash (-).
- Indicates the number of currently learned MAC addresses (forwarding and blocking) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): Click to refresh the port security switch status information manually.

4-7.3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

- 1. Specify the port that you want to monitor.
- 2. Checked "Auto-refresh".



Figure 4-7.3: The Port Security Port Status

Parameter Description

MAC Address & VLAN ID: The MAC address and VLAN ID that are seen on this port. If no MAC addresses are learned, "No MAC Addresses Attached" will display.

State: Indicates whether or not the corresponding MAC address is blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Shows the date and time when this MAC address was first seen on the port.

Age/Hold: If at least one user module decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the port security module will periodically if that this MAC address can still forward traffic. If the aging period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh): Click to refresh the port security port status information manually.

4-8 Access Management

This section configures the access management table of the switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN or over the Internet.

4-8.1 Configuration

This section configures the access management table of the switch. The maximum entry number is 16. If the application's type matched any of access management entries, it will allow access to the switch.

Web Interface

To configure an Access Management Configuration in the web interface:

1. Select "Enabled" in the mode of access management configuration.
2. Click "Add New Entry".
3. Specify the "Start IP Address" and "End IP Address".
4. Checked the "Access Management" method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click "Apply".

Access Management Configuration

Mode: Disabled ▼

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Add new entry					

Apply Reset

Access Management Configuration

Mode: Enabled ▼

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add new entry					

Apply Reset

Figure 4-8.1: The Access Management Configuration

**Parameter
Description**

Mode: Indicates the access management mode operation. Possible modes are:

- **Enabled:** Enable access management mode operation.
- **Disabled:** Disable access management mode operation.

Delete: Check to delete the entry. It will be deleted during the next save.

Start IP address: Indicates the start IP address for the access management entry.

End IP address: Indicates the end IP address for the access management entry.

HTTP/HTTPS: Indicates that the host can access the switch from a HTTP/HTTPS interface, if the host IP address matches the IP address range provided in the entry.

SNMP: Indicates that the host can access the switch from the SNMP interface, if the host IP address matches the IP address range provided in the entry.

TELNET/SSH: Indicates that the host can access the switch from the TELNET/SSH interface, if the host IP address matches the IP address range provided in the entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

4-8.2 Statistics

This section shows the detailed statistics of the access management including HTTP, HTTPS, SSH TELNET, and SSH.

Web Interface

To configure an Assess Management Statistics in the web interface:

- 1. Checked "Auto-refresh".

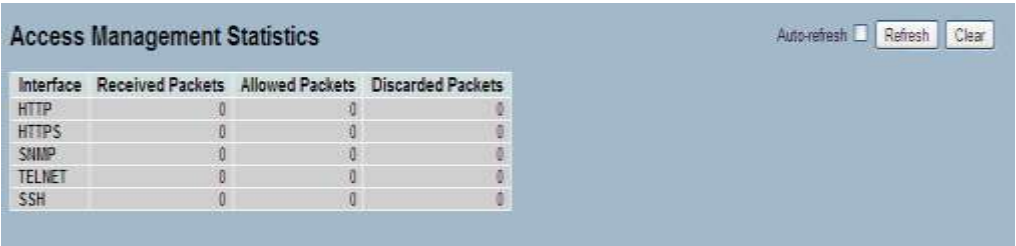


Figure 4-8.2: The Access Management Statistics

Parameter
Description

Interface: The interface type through which the remote host can access the switch.

Received Packets: Number of received packets from the interface when access management mode is enabled.

Allowed Packets: Number of allowed packets from the interface when access management mode is enabled

Discarded Packets: Number of discarded packets from the interface when access management mode is enabled.

Auto-refresh: Evoke the auto-refresh icon to refresh the information automatically.

Upper right icon (Refresh, Clear): Click to refresh or clear the access management statistics information manually.

4-9 SSH

This section shows you to use SSH (Secure SHell) to securely access the switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH Configuration in the web interface:

1. Select “Enabled” in the mode of SSH configuration.
2. Click “Apply”.

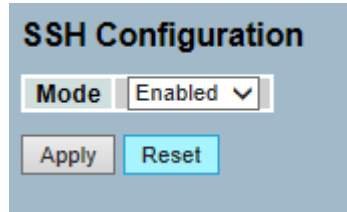


Figure 4-9.1: The SSH Configuration

Parameter Description

Mode: Indicates the SSH mode operation. Possible modes are:

- **Enabled:** Enables the SSH mode operation.
- **Disabled:** Disables the SSH mode operation.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert back to previously saved values.

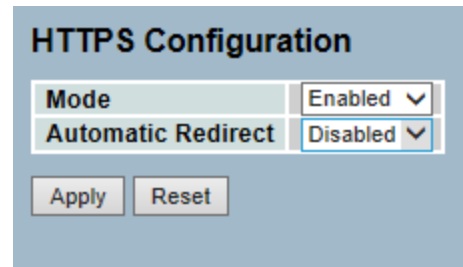
4-10 HTTPS

This section uses HTTPS to securely access the switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS Configuration in the web interface:

1. Select “Enabled” in the mode of HTTPS configuration.
2. Select “Enabled” in the automatic redirect of HTTPS Configuration.
3. Click “Apply”.



HTTPS Configuration	
Mode	Enabled ▼
Automatic Redirect	Disabled ▼
<div>Apply Reset</div>	

Figure 4-10.1: The HTTPS Configuration

Parameter Description

Mode: Indicates the HTTPS mode operation. Possible modes are:

- **Enabled:** Enables the HTTPS mode operation.
- **Disabled:** Disables the HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. Automatically redirect the web browser to HTTPS when the HTTPS mode is enabled. Possible modes are:

- **Enabled:** Enables the HTTPS redirect mode operation.
- **Disabled:** Disables the HTTPS redirect mode operation.

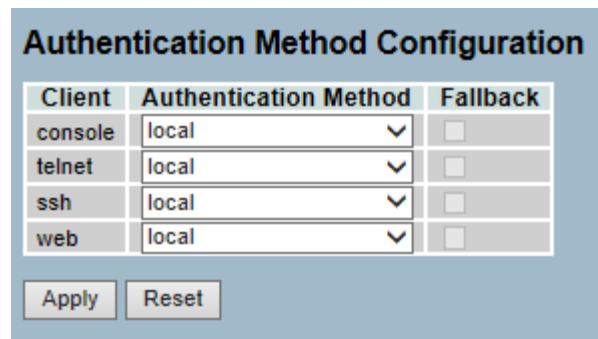
4-11 Auth Method

This page shows how to configure an authenticated user when they log into the switch via one of the management client interfaces.

Web Interface

To configure an Authentication Method Configuration in the web interface:

1. Specify which client (console, telnet, ssh, web) you want to monitor.
2. Specify the "Authentication Method" (none, local, radius, tacacs+).
3. Checked "Fallback".
4. Click "Apply".



Client	Authentication Method	Fallback
console	local	<input checked="" type="checkbox"/>
telnet	local	<input checked="" type="checkbox"/>
ssh	local	<input checked="" type="checkbox"/>
web	local	<input checked="" type="checkbox"/>

Apply Reset

Figure 4-11.1: The HTTPS Configuration

Parameter Description

Client: The management client for which the configuration below applies.

Authentication Method: Authentication method can be set to one of the following values:

- **None:** Authentication is disabled and login is not possible.
- **Local:** Uses the local user database on the switch for authentication.
- **Radius:** Uses a remote RADIUS server for authentication.
- **Tacacs+:** Uses a remote TACACS+ server for authentication.

Fallback: Enables fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the authentication method is set to a value other than "None" or "Local".

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset** – Click "Reset" to undo any changes made locally and revert back to previously saved values.

Chapter 5: Maintenance

5-1 Restart Device

This chapter describes the entire switch maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

It also describes how to restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click “Restart Device”.
2. Click “Yes”.

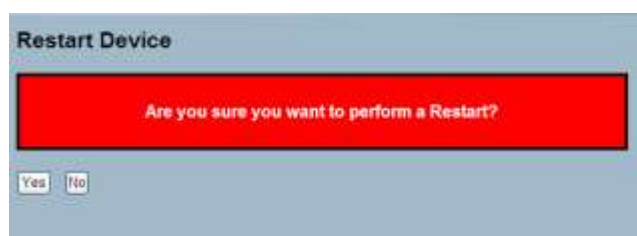


Figure 5-1.1: The Restart Device

Parameter Description

Restart Device: You can restart the switch on this page. After restart, the switch will boot normally.

Buttons:

- **Yes** – Click to “Yes” then the device will restart.
- **No** – Click to undo any restart action.

5-2 Firmware

This section describes how to upgrade the firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5-2.1 Firmware Upgrade

This page facilitates an update of the firmware controlling the switch.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

- 1. Click “Browse” to select the firmware for the device.
- 2. Click “Upload”.



Figure 5-2.1: The Firmware update

Parameter Description

Browse: Click the “Browse...” button to search the firmware URL and filename.

Upload: Click the “Upload” button to upload the firmware.



NOTE: This page facilitates an update of the firmware to control the switch. Uploading the software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page will announce that the firmware update is initiating. After about a minute, the firmware is updated and all managed switches will restart.



WARNING: While the firmware is being updated, web access will appear to be defunctional. The front LED will flash Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

5-2.2 Firmware Selection

The switch supports dual image for firmware redundancy purpose. You can select the firmware image for the device’s start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device and allows you to switch to the alternate image.

Web Interface

To configure a Firmware Selection in the web interface:

- 1. Click “Activate Alternate Image”.
- 2. Click “Yes” to complete the firmware selection.

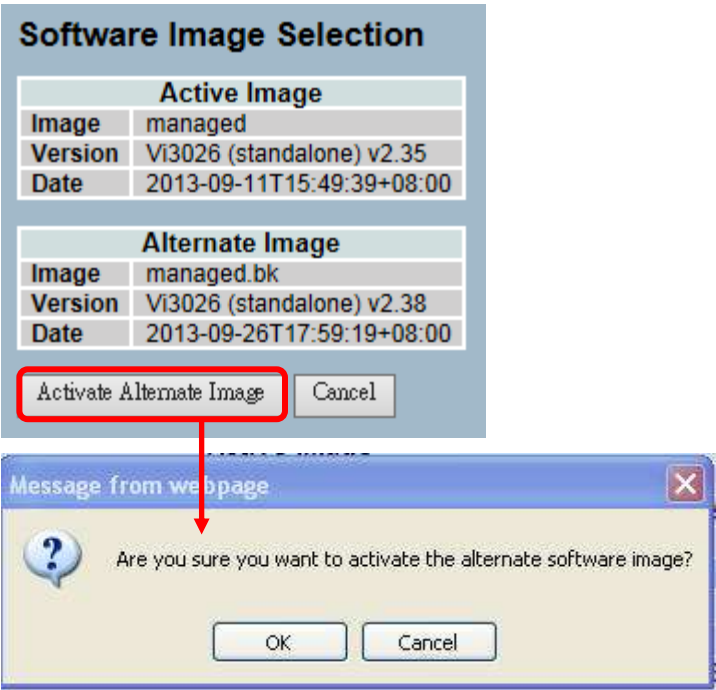


Figure 5-2.2: The Firmware Selection

Parameter Description

Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancels the backup image. Navigates away from this page.

Image: The flash index name of the firmware image. The name of primary (preferred) image is “image”. The alternate image is named “image.bk”.

Version: The version of the firmware image.

Date: The date where the firmware was produced.



NOTE:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the "Activate Alternate Image" button is also disabled.
 2. If the alternate image is active (due to a corruption of the primary image or manually intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
 3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.
-

5-3 Save/Restore

This section describes how to save and restore the switch configuration including reset to Factory Defaults, Save Start, Save Users, and Restore Users for any maintenance needs.

5-3.1 Factory Defaults

This section describes how to reset the switch configuration to factory defaults. Any configuration files or scripts will be reverted to factory default values.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Click “Factory Defaults”.
2. Click “Yes”.



Figure 5-3.1: The Factory Defaults

Parameter Description

Buttons:

- **Yes** – Click to “Yes” button to reset the configuration to Factory Defaults.
- **No**- Click to return to the port state page without resetting the configuration.

5-3.2 Save Start

This section describes how to save the switch start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save Start Configuration in the web interface:

1. Click "Save Start".
2. Click "Yes".



Figure 5-3.2: The Save Start Configuration

Parameter Description

Buttons:

- **Save** – Click the "Save" button to save current setting as start configuration.

5-3.3 Save User

This section describes how to save users information. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save User Configuration in the web interface:

1. Click “Save User”.
2. Click “Yes”.

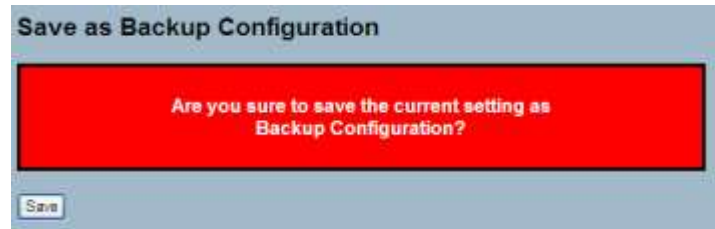


Figure 5-3.3: The Save as Backup Configuration

Parameter Description

Buttons:

- **Save** – Click the “Save” button to save current setting as backup configuration.

5-3.4 Restore User

This section describes how to restore users' information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a Restore User Configuration in the web interface:

1. Click "Restore User".
2. Click "Yes".



Figure 5-3.4: The Restore the Backup Configuration

Parameter Description

Buttons:

- **Save** – Click the "Save" button to restore the Backup Configuration to the switch.

5-4 Export/Import

This section describes how to export and import the switch configuration. Any current configuration files will be exported as XML format.

5-4.1 Export Config

This section describes how to export the switch configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Export Config Configuration in the web interface:

1. Click “Save Configuration”.
2. Save the file in your device.

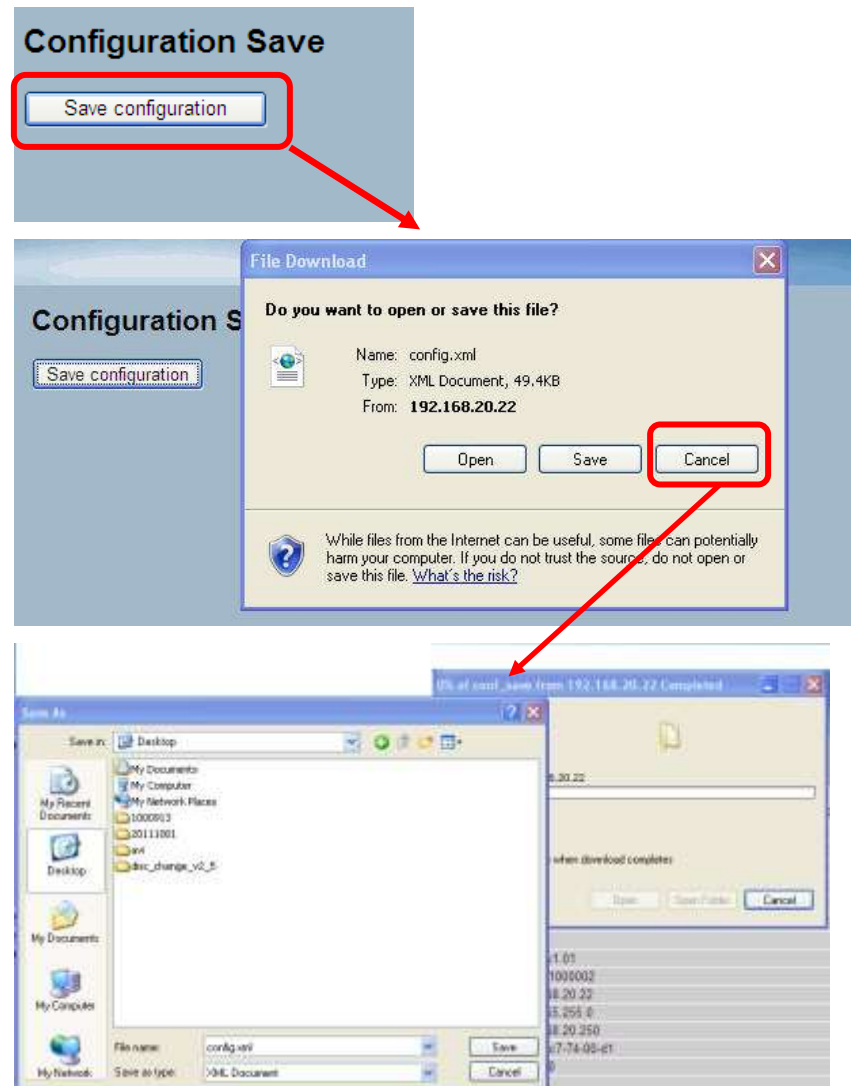


Figure 5-4.1: The Restore the Backup Configuration

Parameter Description

Button:

- **Save** – Click the “Save” button to store the configuration to the PC or server.

5-4.2 Import Config

This section describes how to export the switch configuration for any maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Import Config Configuration in the web interface:

1. Click “Browse” to select the configuration file.
2. Click “Upload”.

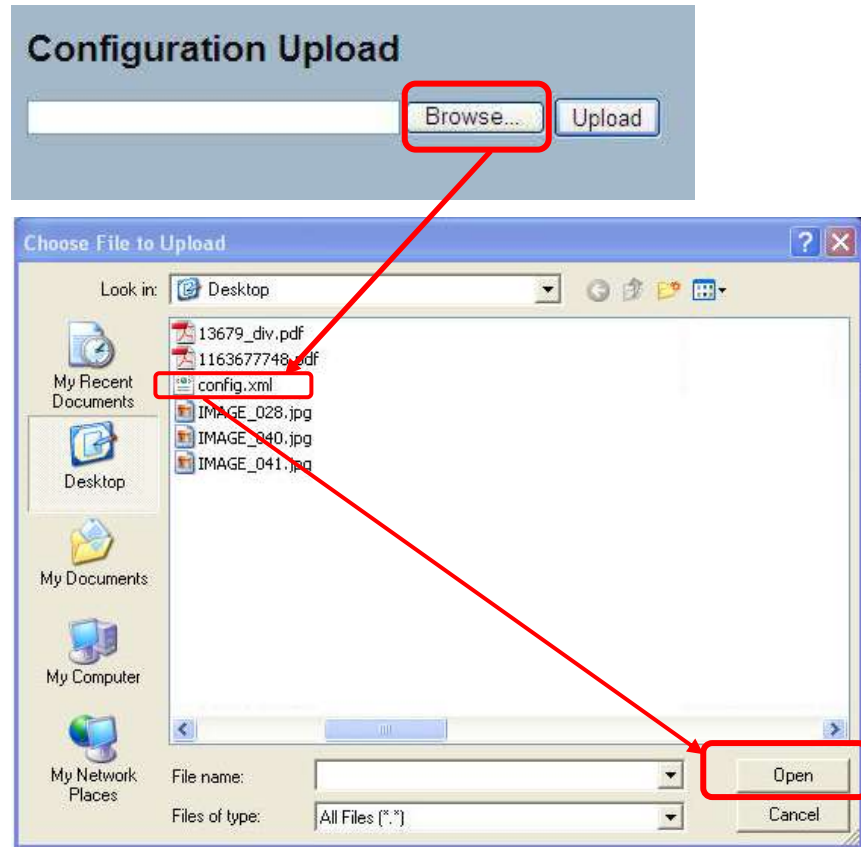


Figure 5-4.2: The Import Config

Parameter Description

Browse: Click the “Browse...” button to search the configuration URL and filename.

Upload: Click the “Upload” button to upload the configuration.

5-5 Diagnostics

This section provides a set of basic system diagnosis. It lets the users know that whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

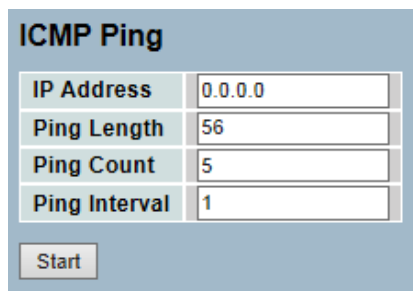
5-5.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Specify the ICMP PING IP Address.
2. Specify the ICMP PING Size.
3. Click “Start”.



ICMP Ping	
IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1
<input type="button" value="Start"/>	

Figure 5-5.1: The ICMP Ping

Parameter Description

IP Address: To set the IP address of the device you want to ping.

Ping Length: The payload size of the ICMP packet. The values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. The values range from 1time to 60 times.

Ping Interval: The interval of the ICMPv6 packet. The values range from 0second to 30 seconds.

Start: Click the “Start” button, then the switch will start to ping the device using ICMP packet size what set on the switch.

After you press “Start”, 5 ICMP packets are transmitted. The sequence number and roundtrip time are displayed once a reply is received. The page refreshes automatically until responses to all packets are received or until a timeout occurs.

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

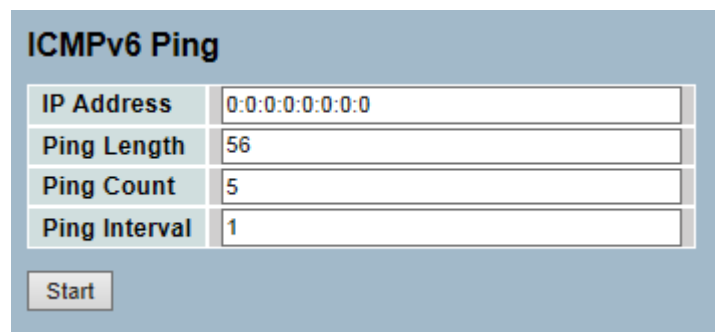
5-5.2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify the ICMPv6 PING IP address.
2. Specify the ICMPv6 PING size.
3. Click “Start”.



ICMPv6 Ping	
IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
<input type="button" value="Start"/>	

Figure 5-5.2: The ICMPv6 Ping

Parameter Description

IP Address: The destination IP Address with IPv6.

Ping Length: The payload size of the ICMP packet. The values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. The values range from 1 time to 60 times.

Ping Interval: The interval of the ICMPv6 packet. The values range from 0 second to 30 seconds.

Start: Click the “Start” button, then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

After you press “Start”, 5 ICMPv6 packets are transmitted and the sequence number and roundtrip time are displayed once a reply is received. The page refreshes automatically until responses to all packets are received or until a timeout occurs.

You can configure the following properties of the issued ICMP packets:

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

5-6 Battery Replacement

It is recommended that only qualified service personnel replace the internal battery.



CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Glossary of Web-based Management

A

Ace

ACE is an acronym for Access Control Entry. It describes the access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed and different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

For example, the ACL implementations can be quite complex when the ACEs are prioritized for the various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES	AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
APS	APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.
Aggregation	Use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability (also Port Aggregation and Link Aggregation).
ARP	ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.
ARP Inspection	ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.
Auto-Negotiation	Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.
C	
CC	CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.
CCM	CCM is an acronym for Continuity Check Message. It is an OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.
CDP	CDP is an acronym for Cisco Discovery Protocol.
D	
DEI	DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
DES	DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS	DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name <code>www.example.com</code> might translate to <code>192.168.0.1</code> .
DoS	DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.
Dotted Decimal Notation	Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form <code>x.y.z.w</code> , where <code>x</code> , <code>y</code> , <code>z</code> , and <code>w</code> are decimal numbers between 0 and 255.
DSCP	DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.
E	
EEE	EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.
EPS	EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.
Ethernet Type	Ethernet Type, or EtherType, is a field in the Ethernet MAC header defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.
F	
FTP	FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
Fast Leave	Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H **HTTP**

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate log-ons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I **ICMP**

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP	IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP Query messages onto a particular link. This router is called the Querier.
IP	<p>IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.</p> <p>IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.</p> <p>The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.</p>
IPMC	IPMC is an acronym for IP MultiCast
IP Source Guard	IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.
L	
LACP	LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.
LLC	The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP	<p>LLDP is an IEEE 802.1ab standard protocol.</p> <p>The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).</p>
LLDP-MED	LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LOC	LOC is an acronym for Loss of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.
M	
MAC Table	<p>Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.</p> <p>The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.</p>
MEP	MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
MD5	MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.
Mirroring	For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port (In this context, mirroring a frame is the same as copying the frame.) Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name. It provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them. This means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs	A LLDP frame contains multiple TLVs. For some TLVs, it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.
OUI	OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.
P	
PCP	PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.
PD	PD is an acronym for Powered Device. In a PoE system, the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.
PHY	PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).
PING	<p>Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.</p> <p>Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.</p>
PoE	PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. It could be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP	PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.
Q	
QCE	QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.
QCI	QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QL	QL in SyncE; this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.
QoS	<p>QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.</p> <p>A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.</p> <p>Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.</p>
R	
RARP	RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.
RADIUS	RADIUS is an acronym for Remote Authentication Dial in User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.
RDI	RDI is an acronym for Remote Defect Indication. It is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP
RSTP	In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP while being backwards-compatible with STP.

S	SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.
SHA	
Shaper	A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.
SMTP	SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.
SNAP	The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.
SNMP	SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.
SNTP	SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to, based on pre-configuration or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).
SSH	SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).
SSM	SSM in SyncE; this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP	Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.
SyncE	SyncE is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).
T	
TACACS+	TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.
Tag Priority	Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.
TCP	<p>TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.</p> <p>The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.</p> <p>The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.</p> <p>Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).</p>
TELNET	TELNET is an acronym for TELeType NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.
TFTP	TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.
U	
UDP	UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN is a method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Contact Information

Vigitron, Inc.

7810 Trade Street, Suite 100

San Diego, CA 92121

support@vigitron.com

Tel: (858) 484-5209

Fax: (858) 484-1205

www.vigitron.com